BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-145356
(43)Date of publication of application : 29.05.1998

(51)Int.Cl. H04L 9/32

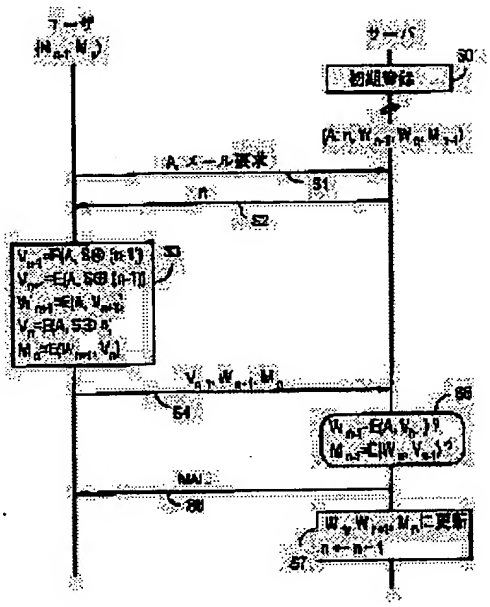
(21)Application number : 09-247133
(22)Date of filing : 11.09.1997

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : SHIMIZU AKIHIRO
HORIOKA TSUTOMU
HAMADA HIROSHI

(30)Priority
Priority number : 08240190 Priority date : 11.09.1996 Priority country : JP

(54) INFORMATION TRANSMITTING AND RECEIVING CONTROL METHOD WITH USER IDENTIFYING FUNCTION AND RECORDING MEDIUM RECORDING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To dispense with the read/write of a storing medium by the side of a person to be identified and to safely execute user identifying processing by a small program size by initially register the initial values and the identification A of identification data of this time and a time after next and its propriety inspecting data Wn-1, Wn +1 and Mn, allowing both of a user and a server to calculate through the use of a unidirectional function each time of the identifying request of the user and identifying the user, when these data to increment match.
SOLUTION: E is the unidirectional function, and S is a password which the user holds secretly. (+) is exclusive OR. The user initially registers V0=E(A, S), W0=E(A, V0), V1=E(A, S(+)1), W1=E(A, V1), M0=E(W1, V0). The server calculates Vn-1=E(A, S(+)(n-1)), Vn=E(A, S(+)n), Vn+1=E(A, S(+)(n+1)), Wn+1=E(A, Vn+1), Mn=E(Wn+1, Vn) as an n-th identification value and compares it with a value received from the user.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平１０－１４５３５６

(43)公開日　平成１０年（１９９８）５月２９日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
H04L 9/32			H04L 9/00	675 A	
				673 A	
				673 C	
				673 D	

審査請求　未請求　請求項の数２０　ＯＬ　（全２０頁）

(21)出願番号　特願平９－２４７１３３

(22)出願日　平成９年（１９９７）９月１１日

(31)優先権主張番号　特願平８－２４０１９０

(32)優先日　平８（１９９６）９月１１日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　０００００４２２６
日本電信電話株式会社
東京都新宿区西新宿三丁目１９番２号

(72)発明者　清水　明宏
東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

(72)発明者　堀岡　力
東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

(72)発明者　浜田　洋
東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

(74)代理人　弁理士　草野　卓

(54)【発明の名称】ユーザ認証機能を有する情報送受信制御方法及びその方法を記録した記録媒体

(57)【要約】

【課題】　被認証者側に記憶媒体の読み書きを行う機構を必要とせず、かつユーザ認証処理を小さいプログラムサイズで安全に行う。

【解決手段】　ユーザはｎ=0，メールアカウントＡ，パスワードＳを設定し、一方向性関数$V_0=E(A, S)$、$W_0=E(A, V_0)$，$V_1=E(A, A(+)1)$，$W_1=E(A, V_1)$，$M_0=E(W_1, V_0)$を求め、W_0，W_1，M_0，Ａを電子メールでメールサーバに初期登録しておく。出先でユーザは電子メールにか加入している任意の端末を用い、サービス起動要求とＡをメールサーバに送り、メールサーバは識別子Ａの認証回数ｎを読みだし、それを返送する。ユーザは$V_{n-1}=E(A, S(+)(n-1))$，$V_{n+1}=E(A, S(+)(n+1))$，$W_{n+1}=E(A, V_{n+1})$，$V_n=E(A, S(+)n)$，$M_n=E(W_{n+1}, V_n)$を求めてV_{n-1}，W_{n+1}，M_nをメールサーバに送る。メールサーバは、$E(A, V_{n-1})$，$E(W_n, V_{n-1})$を求め、登録されているデータW_{n-1}，M_{n-1}とそれぞれ一致すれば、ＯＫとしてそのユーザのメールメッセージを送る。

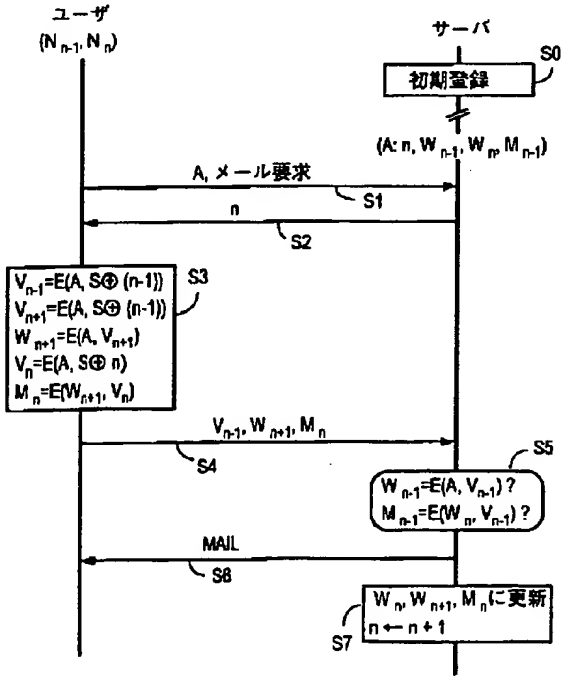


図３

1

【特許請求の範囲】

【請求項１】　ネットワーク上でユーザが利用するユーザ端末装置と、認証者の認証者装置との間で認証処理を行うための情報送受信制御方法であり、以下のステップを含む：

(a) 初期登録手順として、上記ユーザが、自分の識別子Ａと、秘密に保持しているパスワードＳから、次回認証データW_0、次々回認証データW_1、上記次々回認証データW_1の正当性検証データM_0の３つを算出し、認証回数ｎの初期値n=1 と共に上記認証者装置に上記識別子Ａと対応して登録し、

(b) 次に、ｎを正の整数とすると、第ｎ回目の認証において、上記認証者装置は、上記ユーザ端末装置からサービス起動要求と上記ユーザの識別子Ａの通知を受けて、そのユーザの認証回数ｎを読みだし、そのユーザ端末装置へ通知し、

(c) 上記ユーザ端末装置では、上記ユーザの識別子Ａ、送られてきた上記認証回数ｎ及び秘密に保持しているパスワードＳを用いて、今回の被認証データV_{n-1}、次々回の認証データW_{n-1}、次々回認証データW_{n-1}の正当性検証データM_nを算出し、送信したいコンテンツデータがある場合にはそのデータと共に上記認証者装置に通知し、

(d) 上記認証者装置では、上記ユーザの識別子Ａと上記ステップ(c) で送付されてきた今回の被認証データV_{n-1}とから算出した今回の認証データW_{n-1}を、登録されている認証データW_{n-1}と比較し、かつ登録されている次回認証データW_nと、上記今回の被認証データV_{n-1}とから計算した正当性検証データM_{n-1}を、登録されている正当性検証データM_{n-1}と比較し、

(e) 上記ステップ(d) の比較の結果、一致した場合、上記認証者装置ではそのユーザを正当とし、上記ユーザが要求したサービス情報の送受信を行うとともに、前回受けた次回認証データW_nと、今回送付されてきた次々回認証データW_{n+1}、と次々回認証データの正当性検証データM_nを、前回登録したW_{n-1}, W_n, M_{n-1}と置き換えて登録し、認証回数ｎをインクリメントし、

(f) 上記ステップ(d) の比較の結果、一致しない場合、そのユーザを不当とし以降の情報送受信を拒否し、前回登録したデータW_{n-1}, W_n, M_n及びｎをそのまま保持する。

【請求項２】　請求項１の方法において、上記ユーザは上記認証者装置において上記ステップ(a) の初期登録手順を実行する。

【請求項３】　請求項１の方法において、上記ユーザ端末装置と認証者装置間のデータ送受信に、電子メールプロトコルを用い、通信処理のコンテンツデータを上記ユーザ宛の電子メールとし、認証者装置にある上記ユーザの電子メール情報を遠隔地にある上記ユーザ端末装置へ転送したり、あるいは、上記ユーザのメールアドレスで遠隔地から電子メールの発信を行う。

2

【請求項４】　請求項１の方法において、上記ユーザは、上記ユーザ端末装置において上記データW_0, W_1, M_0を生成し、上記認証回数初期値n=1 と共に上記認証者装置に送信することにより上記ステップ(a) の初期登録手順を実行する。

【請求項５】　請求項４の方法において、上記認証者装置は、上記ステップ(b) において上記ステップ(c) のユーザ側認証手順を特定の通信単位に予め決められた方法で記述したプログラムの通信単位を上記ユーザ端末装置へ送り込み、上記ステップ(c) において上記ユーザ端末装置はその送り込まれた通信単位プログラムを実行することにより認証手順を実行する。

【請求項６】　請求項４の方法において、上記認証者装置は、上記ステップ(a) の前にユーザの要求に応じて上記ステップ(a) の初期登録手順を特定の通信単位に予め決められた方法で記述したプログラムの通信単位を上記ユーザ端末装置へ送り込み、上記ステップ(a) において上記ユーザ端末装置はその通信単位プログラムを実行することにより上記初期登録手順を実行する。

【請求項７】　請求項１又は４の方法において、(+) を排他的論理和、Ｅを一方向性関数とすると、上記ステップ(a)は次の手順

$V_0 = E(A, S)$

$W_0 = E(A, V_0)$

$V_1 = E(A, S(+)1)$

$W_1 = E(A, V_1)$

$M_0 = E(W_1, V_0)$

で上記データ初期値W_0, W_1, M_0を算出し、上記ステップ(c) は次の手順

$V_{n-1} = E(A, S(+)(n-1))$

$V_n = E(A, S(+)n)$

$V_{n+1} = E(A, S(+)(n+1))$

$W_{n+1} = E(A, V_{n+1})$

$M_n = E(W_{n+1}, V_n)$

で上記認証用データV_{n-1}, W_{n+1}, M_nを算出し、上記ステップ(d) は上記ユーザから受信したデータV_{n-1}と、登録されているデータA, W_nとから$E(A, V_{n-1})$と$E(W_n, V_{n-1})$を計算し、それらが登録されているデータW_{n-1}とM_{n-1}にそれぞれ一致するかを判定する。

【請求項８】　請求項１の方法において、上記ネットワークは上記ユーザ端末装置が接続されたインタネットと、そのインタネットに接続されたイントラネットを含み、上記認証者装置は上記イントラネット上に接続して設けられており、上記インタネット上に公開された中継サーバが接続して設けられており、上記ユーザと上記中継サーバとの間では高速通信プロトコルを使って送受信が行われ、上記中継サーバと上記認証装置との間では電子メールプロトコルを使って送受信が行われ、それによって、上記ユーザ端末装置と上記認証装置間での認証情報のやりとりを上記中継サーバを介して行う。

3

【請求項９】　請求項８の方法において、上記ユーザは上記ステップ(c)において上記データV_{n-1}, W_{n+1}, M_nを送出後、一旦上記中継サーバとの接続を切断し、上記認証者装置は上記ステップ(e)において認証が完了した時点で、上記ユーザが要求したサービスの情報を上記中継サーバに転送し、そこに保管し、上記ユーザは、上記中継サーバとの接続を切断してから一定時間が経過した後の任意の時間に上記中継サーバに再度接続し、上記中継サーバとの間で上記サービス情報に対する上記ユーザの正当性を検証する認証処理を行い、上記サービス情報を受信する。

【請求項１０】　インタネットにユーザ端末装置と中継サーバがそれぞれ接続されており、そのインタネットに接続されたイントラネットに認証者装置が接続されており、上記ユーザ端末装置と上記認証者装置との間の情報送受信を上記中継サーバを介して行う場合に、上記ユーザ端末装置と上記中継サーバ間は高速通信プロトコルを使って行い、上記中継サーバと上記認証者装置間は電子メールプロトコルを使って行うシステムにおける、上記ユーザと認証者との間で認証処理を行うための情報送受信制御方法であり、以下のステップを含む：

(a) 上記ユーザの識別子Ａと、秘密に保持しているパスワードＳから、次回認証データW_0、次々回認証データW_1、上記次々回認証データW_1の正当性検証データM_0の３つを算出し、上記認証者装置に上記識別子Ａと対応して登録し、上記認証回数ｎの初期値n=1 を上記認証者装置と上記中継サーバにそれぞれ上記識別子Ａと対応させて保持し、

(b) ｎを正の整数とすると、第ｎ回目の認証において、上記中継サーバは上記ユーザ端末装置からサービス要求と識別子Ａを受けると、対応する認証回数ｎを読みだし、上記ユーザ端末装置に送り、

(c) 上記ユーザ端末装置では、上記ユーザの識別子Ａ、送られてきた上記認証回数ｎ及び秘密に保持しているパスワードＳを用いて、今回の被認証データV_{n-1}、次々回の認証データW_{n+1}、その次々回認証データW_{n+1}の正当性検証データM_nを算出し、送信したいコンテンツデータがある場合にはそのデータと共に上記中継サーバを介して上記認証者装置に送り、その後上記中継サーバとの接続を一旦切断し、

(d) 上記認証者装置では、上記ユーザの識別子Ａと上記ステップ(c)で送付されてきた今回の被認証データV_{n-1}とから算出した今回の認証データW_{n-1}を、登録されている認証データW_{n-1}と比較し、かつ登録されている次回認証データW_nと、上記今回の被認証データV_{n-1}とから計算した正当性検証データM_{n-1}を、登録されている正当性検証データM_{n-1}と比較し、

(e) 上記ステップ(d)の比較の結果、一致した場合、上記認証者装置では、そのユーザを正当とし、上記ユーザが要求したサービスの情報を上記中継サーバに転送して、そこに保管し、或いは、送信したいコンテンツ情報がある場合には、認証されたユーザの資格でその情報の送信を行い、送信を完了したことを示す確認情報を中継サーバに送信し、

(f) 上記認証者装置は更に、前回受けた次回認証データW_nと、今回送付されてきた次々回認証データW_{n+1}、と次々回認証データの正当性検証データM_nを、前回登録したデータW_{n-1}, W_n, M_{n-1}と置き換えて登録し、認証回数ｎをインクリメントし、上記ステップ(d)の比較の結果、一致しない場合、そのユーザを不当とし以降の情報送受信を拒否し、前回登録したW_{n-1}, W_n, M_n及びｎをそのまま保持し、

(g) 上記中継サーバは、上記サービス情報或いは上記送信確認情報を受け取った後、上記認証回数ｎをインクリメントし、

(h) 上記ユーザは、上記中継サーバとの接続を切断してから一定時間が経過した後の任意の時間に上記中継サーバに再度接続し、上記中継サーバとの間で上記サービス情報に対する上記ユーザの正当性を検証する認証処理を行い、上記サービス情報を受信する。

【請求項１１】　請求項９又は１０の方法において、

(+) を排他的論理和、Ｅを一方向性関数、上記認証者装置の識別子をA_nとすると、上記ステップ(a)では上記初期登録のための上記３つのデータW_0, W_1, M_0を次の手順

$V_0 = E(A(+)A_n, S)$

$W_0 = E(A(+)A_n, V_0)$

$V_1 = E(A(+)A_n, S(+)1)$

$W_1 = E(A(+)A_n, V_1)$

$M_0 = E(W_1, V_0)$

により求め、上記ユーザは上記第ｎ回目の認証における上記データV_{n-1}, W_{n+1}, M_nを次の手順

$V_{n-1} = E(A(+)A_n, S(+)(n-1))$

$V_n = E(A(+)A_n, S(+)n)$

$V_{n+1} = E(A(+)A_n, S(+)(n+1))$

$W_{n+1} = E(A(+)A_n, V_{n+1})$

$M_n = E(W_{n+1}, V_n)$

により求め、上記認証者装置は上記比較をする処理を$W_{n-1}=E(A(+)A_n, V_{n-1})$の一致と、$M_{n-1}=E(W_n, V_{n-1})$の一致を検証することによって行う。

【請求項１２】　請求項１１の方法において、上記ユーザと上記中継サーバ間の認証は、その認証回数をｎ’とし、上記中継サーバの識別子をA_nとすると、以下のステップを含む：

(a’)　初期登録手順として、上記ユーザが、一方向性関数Ｅを使って自分の識別子Ａと、秘密に保持しているパスワードＳから、次回認証データW_0、次々回認証データW_1、次々回認証データW_1の正当性検証データM_0の３つを算出し、認証回数ｎ’の初期値n’=1と共に上記中継サーバに上記識別子Ａと対応して登録し、

(b’)　次に、ｎ’を正の整数とすると、第ｎ’回目の認

4

5

証において、上記中継サーバは、上記ユーザ端末装置からサービス要求と上記ユーザの識別子Ａの通知を受けて、そのユーザの認証回数ｎ' を読みだし、そのユーザ端末装置へ通知し、

(c') 上記ユーザ端末装置では、上記ユーザの識別子Ａ、送られてきた上記認証回数ｎ' 及び秘密に保持しているパスワードＳを用いて、今回の被認証データ$V_{n'-1}$、次々回の認証データ$W_{n'+1}$、次々回認証データ$W_{n'+1}$の正当性検証データ$M_{n'}$を算出し、

(d') 上記中継サーバでは、上記ユーザの識別子Ａと上記ステップ(c')で送付されてきた今回の被認証データ$V_{n'-1}$とから算出した今回の認証データ$W_{n'-1}$を、登録されている認証データ$W_{n'-1}$と比較し、かつ登録されている次回認証データ$W_{n'}$と、上記今回の被認証データ$V_{n'-1}$とから計算した正当性検証データ$M_{n'-1}$を、登録されている正当性検証データ$M_{n'-1}$と比較し、

(e') 上記ステップ(d')の比較の結果、一致した場合、そのユーザを正当とし、上記ユーザが要求したサービスの情報送受信を行うとともに、前回受けた次回認証データ$W_{n'}$と、今回送付されてきた次々回認証データ$W_{n'+1}$、と次々回認証データの正当性検証データ$M_{n'}$を、前回登録した$W_{n'-1}$, $W_{n'}$, $M_{n'-1}$と置き換えて登録し、認証回数ｎ' をインクリメントする。

【請求項１３】 請求項１２の方法において、上記ステップ(a')は上記次回認証データW_0、次々回認証データW_1、次々回認証データW_1の正当性検証データM_0を次式

$V_0 = E(A(+)A_x, S)$

$W_0 = E(A(+)A_x, V_0)$

$V_1 = E(A(+)A_x, S(+)1)$

$W_1 = E(A(+)A_x, V_1)$

$M_0 = E(W_1, V_0)$

により計算し、上記ステップ(b')は上記今回の被認証データ$V_{n'-1}$、次々回の認証データ$W_{n'+1}$、次々回認証データ$W_{n'+1}$の正当性検証データ$M_{n'}$を次式

$V_{n'-1} = E(A(+)A_x, S(+)(n'-1))$

$V_{n'} = E(A(+)A_x, S(+)n')$

$V_{n'+1} = E(A(+)A_x, S(+)(n'+1))$

$W_{n'+1} = E(A(+)A_x, V_{n'+1})$

$M_{n'} = E(W_{n'+1}, V_{n'})$

により計算し、上記ステップ(d')は今回の認証データ$W_{n'-1}=E(A(+)A_x, V_{n'-1})$を、登録されている認証データ$W_{n'-1}$と比較し、かつ登録されている次回認証データ$W_{n'}$と、上記今回の被認証データ$V_{n'-1}$とから計算した正当性検証データ$M_{n'-1}=E(W_{n'}, V_{n'-1})$を、登録されている正当性検証データ$M_{n'-1}$と比較する。

【請求項１４】 ユーザ端末装置と、サービスプロバイダと、認証者装置とがインタネットに接続されており、ユーザがインタネット上でサービスプロバイダからサービスを受ける場合に、ユーザが認証者装置との間で認証処理を行うための情報送受信制御方法であり、以下のステップを含む：

6

(a) 初期登録手順として、上記ユーザのアカウントＡと、パスワードＳから次回認証データW_0、次々回認証データW_1、上記次々回認証データW_1の正当性検証データM_0の３つを計算し、認証回数初期値n=1 と、金額Ｘと共に上記アカウントＡと対応して登録し、

(b) ユーザは上記サービスプロバイダに所望のサービスを要求するサービス要求信号とアカウントＡを送り、

(c) 上記サービスプロバイダは受信した上記アカウントＡを上記課金管理センタに転送し、

(d) 上記課金管理センタは上記アカウントＡに対応する認証回数ｎを読み出し、上記サービスプロバイダに送り、

(e) 上記サービスプロバイダは受信した認証回数ｎを認証手順のAppletプログラムと共にユーザ端末装置に送り、

(f) 上記ユーザは上記認証手順に従って認証用データ$V_{n'-1}$, $W_{n'+1}$, $M_{n'}$を計算し、上記アカウントＡと共に上記サービスプロバイダに送り、

(g) 上記サービスプロバイダはデータ$V_{n'-1}$, $W_{n'+1}$, $M_{n'}$と共に上記サービスプロバイダのアカウントA_Pと、上記サービスに対する金額ｘを上記課金管理センタに送り、

(h) 上記認証者装置は上記サービス金額ｘが上記アカウントＡに対応して登録されている残額Ｘ以下であることを確認し、受信したデータ$V_{n'-1}$と登録されている次回認証データ$W_{n'}$を検証し、両方とも正しければ認証確認信号OKを上記サービスプロバイダに送ると共に、データ$W_{n'}$, $W_{n'+1}$, $M_{n'}$に更新し、認証回数ｎをインクリメントし、上記アカウントＡの残額ＸをX-x で更新し、上記プロバイダのアカウントA_Pの残額XPをX_P+xで更新し、

(i) 上記サービスプロバイダは、上記確認信号OKを受けると上記ユーザに上記指定されたサービスを提供する。

【請求項１５】 ネットワーク上でユーザの正当性を認証するための情報送受信制御を行う認証者装置であり、以下を含む：ｎを正の整数とすると、次回認証データ$W_{n'-1}$、次々回認証データ$W_{n'}$、上記次々回認証データ$W_{n'}$の正当性検証データ$M_{n'-1}$を認証回数ｎと共に上記識別子Ａと対応して第n-1 回目の認証時に登録した登録データ記憶手段と、

第ｎ回目の認証において、上記ユーザの端末装置からサービス起動要求と上記ユーザの識別子Ａの通知を受けて、そのユーザの認証回数ｎを上記登録データ記憶手段から読みだし、そのユーザ端末装置へ通知する認証回数送出手段と、

上記ユーザ端末装置から送られてきた今回の被認証データ$V_{n'-1}$、次々回の認証データ$W_{n'+1}$、上記次々回認証データ$W_{n'+1}$の正当性検証データ$M_{n'}$を受信する受信手段と、

上記ユーザの識別子Ａと上記受信した今回の被認証データ$V_{n'-1}$とから算出した今回の認証データ$W_{n'-1}$を、上記登録データ記憶手段に登録されている認証データ$W_{n'-1}$と比

7

較し、かつ登録されている次回認証データW_nと、上記今回の被認証データV_{n-1}とから計算した正当性検証データM_{n-1}を、登録されている正当性検証データM_{n-1}と比較する認証手段と、及び上記認証手段による比較の結果、一致した場合、そのユーザを正当とし、登録されている次回認証データW_nと、今回受信した次々回認証データW_{n+1}と、及び今回受信した次々回認証データの正当性検証データM_nとを、上記登録データ記憶手段に登録されているデータW_{n-1}, W_n, M_{n-1}と置き換えて登録し、認証回数ｎをインクリメントする登録更新手段。

【請求項１６】　請求項１５の装置において、上記認証手段は、上記ユーザから受信したデータV_{n-1}と、登録されているデータＡ，W_nとから一方向性関数$E(A, V_{n-1})$と$E(W_n, V_{n-1})$を計算し、それらが登録されているデータW_{n-1}とM_{n-1}にそれぞれ一致するかを判定する手段を含む。

【請求項１７】　ネットワーク上で認証者からユーザに対する認証得るための情報送受信制御を行うユーザ端末装置であり、以下を含む：認証者装置から認証回数ｎを受信する認証回数受信手段と、

上記ユーザの識別子Ａ、受信した上記認証回数ｎ及び秘密に保持しているパスワードＳを用いて、今回の被認証データV_{n-1}、次々回の認証データW_{n+1}、上記次々回認証データW_{n+1}の正当性検証データM_nをそれぞれ認証用データとして計算する認証用データ計算手段と、

上記認証用データを上記認証者装置に送信する認証用データ送信手段。

【請求項１８】　請求項１７の装置において、(+) を排他的論理和とすると、上記認証用データ計算手段は、次の一方向性関数

$V_{n-1} = E(A, S(+)(n-1))$

$V_n = E(A, S(+)n)$

$V_{n+1} = E(A, S(+)(n+1))$

$W_{n+1} = E(A, V_{n+1})$

$M_n = E(W_{n+1}, V_n)$

により上記認証用データV_{n-1}, W_{n+1}, M_nを算出する手段である。

【請求項１９】　ネットワーク上でユーザの正当性を認証する認証者側の認証手順を記録した記録媒体であり、上記認証手順は以下を含む：

(a) (+) を排他的論理和とすると、ユーザの識別子ＡとパスワードＳを使って次の一方向性関数

$V_0 = E(A, S)$

$W_0 = E(A, V_0)$

$V_1 = E(A, S(+)1)$

$W_1 = E(A, V_1)$

$M_0 = E(W_1, V_0)$

によりデータ初期値W_0, W_1, M_0を算出して登録し、

(b) ｎを正の整数とすると、第ｎ回目の認証において、上記ユーザの端末装置からサービス起動要求と上記ユーザの識別子Ａの通知を受けて、そのユーザの認証回数ｎを上記登録データ記憶手段から読みだし、そのユーザ端末装置へ送信し、

(c) 上記ユーザ端末装置から送られてきた今回の被認証データV_{n-1}、次々回の認証データW_{n+1}、その次々回認証データW_{n+1}の正当性検証データM_nを受信し、

(d) 上記ユーザの識別子Ａと上記受信した今回の被認証データV_{n-1}とから一方向性関数$W_{n-1}=E(A, V_{n-1})$により今回の認証データW_{n-1}を算出し、上記登録データ記憶手段に登録されている認証データW_{n-1}と比較し、かつ登録されている次回認証データW_nと、上記今回の被認証データV_{n-1}とから一方向性関数$M_{n-1}=E(W_n, V_{n-1})$により正当性検証データM_{n-1}を算出し、登録されている正当性検証データM_{n-1}と比較し、

(e) ２つの比較結果が同時に一致であった場合、そのユーザを正当とし、登録されている次回認証データW_nと、今回受信した次々回認証データW_{n+1}と、及び今回受信した次々回認証データW_{n+1}の正当性検証データM_nとを、上記登録データ記憶手段に登録されているデータW_{n-1}, W_n, M_{n-1}と置き換えて登録し、認証回数ｎをインクリメントする。

【請求項２０】　ネットワーク上で認証者からユーザに対する認証を得るユーザ側の手順を記録した記録媒体であり、上記手順は、以下を含む：

(a) サービス要求とユーザの識別子Ａを上記認証者装置に送信し、

(b) ｎを正の整数とすると、上記認証者装置から認証回数ｎを受信し、

(c) (+) を排他的論理和とすると、上記ユーザの識別子Ａ、受信した上記認証回数ｎ及び秘密に保持しているパスワードＳを用いて、今回の被認証データV_{n-1}、次々回の認証データW_{n+1}、上記次々回認証データW_{n+1}の正当性検証データM_nを次の一方向性関数

$V_{n-1} = E(A, S(+)(n-1))$

$V_n = E(A, S(+)n)$

$V_{n+1} = E(A, S(+)(n+1))$

$W_{n+1} = E(A, V_{n+1})$

$M_n = E(W_{n+1}, V_n)$

により算出し、上記認証者装置に送信する。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、特に、インタネットのように容易に盗聴され易い、つまり安全性（セキュリティ）が十分でないネットワークにおいて、高速で小規模のプログラムでパスワードを用いたユーザ認証を行い、安全に情報の送受信を実現することのできる情報送受信制御方法（プロトコル）に関するものである。

【０００２】

【従来の技術】インタネットの普及に伴い、通信の際に、通信相手やユーザの資格を認証することが不可欠に

9

なってきている。認証方法には様々な技術が存在するが、大きく分けて、公開鍵暗号方法を応用したものと共通鍵暗号方法を応用したものの二つに分類することができる。

【０００３】このうち、公開鍵暗号方法を用いる方法は、その性質上、優れた認証能力を有しており、電子取引などへの応用が期待されている。しかし、処理に時間がかかり、また、プログラムサイズが大きいため、ＰＤＡ（Personal Digital Assistant：携帯端末）等の処理能力の低い端末やインタネット関連の通信プロトコルなどへの組み込みにおいては、その適用領域が制限されるという問題がある。

【０００４】そこで、このような適用域には、公開鍵暗号方法より格段の高速処理が可能な共通鍵系の暗号方法を応用した方法、特に、パスワード認証方法がよく用いられる。基本的なパスワード認証の手順は以下の通りである。まず、被認証者が認証者にパスワードを登録する。認証時に、被認証者が認証者にパスワードを送信する。認証者は、受信したパスワードと登録されているパスワードを比較する。

【０００５】この方法には、次のような問題点がある。
(a) 認証側にあるパスワードファイルの盗見により、パスワードが盗まれる。
(b) 通信中、回線盗聴によってパスワードが盗まれる。
(c) 被認証者は認証者に、自分の秘密情報であるパスワードを公開する必要がある。

【０００６】最初の問題(a)を解決する方法として、被認証者が認証者側に、パスワードに一方向性関数を施したデータを登録しておき、認証時に、認証者が受信したパスワードに同じ一方向性関数を施し、結果を比較するという方法（参考文献：A.Evans,W.Kantrowitz and E.Weiss："A user authentication scheme not requiring secrecy in the computer," Commun. ACM, 17, 8, pp.437-442(1974)及びR.Morris and K.Thompson:"Password security: A case history," UNIX Programmer's Manual , Seventh Edition , 2B(1979)）がある。

【０００７】一方向性関数とは、入力の総当たり以外に、出力から入力を得る効率的な手段が存在しない関数であり、総当たりの計算量を充分大きくしておけば、無資格者が入力データを算出して被認証者になりすますことを防ぐことができる。一般に、一方向性関数は、ＤＥＳやＦＥＡＬなどの共通鍵暗号方法によって得ることができる。共通鍵暗号方法は、共通秘密鍵を用いて入力される平文を処理して暗号文を出力として得るもので、平文と暗号文が与えられても共通秘密鍵が算出できない。即ち、共通秘密鍵は鍵の総当たりより効率的に得る手段がないように設計されている。したがって、この手法により平文と任意のパラメータ、共通秘密鍵を入力、暗号文を出力とすることによって、共通鍵暗号方法の強さに依存した一方向性関数を実現することができる。更に、

10

ＤＥＳ，ＦＥＡＬなどの共通鍵暗号方法は、平文や共通秘密鍵の入力が１ビット変化しただけでも、その入力変化の痕跡をまったくとどめない出力を得ることができるという特徴を有している。

【０００８】以上説明した通り、一方向性関数を用いた方法によって、基本的なパスワード認証方法の最初に指摘した問題は解決できる。しかし、これを回線盗聴が簡単なインタネットに適用する場合、問題(b)を解決することはできない。また、問題(c)で指摘したように、この基本的なパスワード認証方法は、銀行の顧客認証などには適用できても、同一レベルのユーザ同士の認証には適していない。

【０００９】このような問題を解決する方法として、Lamportの方法（L.Lamport: "Password authentication with insecure communication," Commun. ACM, 24, 11, pp.770-772(1981)），及びこの出願の発明者が提案した動的パスワード認証方法であるCINON法(Chained One-way Data Verification Method) (A.Shimizu, "A Dynamic Password Authentication Method Using a One-way Function" Systtems and Computers in Japan, Vol. 22, No.7, 1991, pp.32-40）がある。

【００１０】Lamportの方法は、パスワードに一方向性関数を複数回適用しておいて、適用一回前のデータを次々と認証者側に示すことで、複数回の認証を可能にする方法である。この方法では、最初に設定した最大認証回数から認証を実行する毎に１を減算し、認証回数を使い尽くした時点で、パスワードを再設定する必要がある。最大認証回数を増やすために一方向性関数の適用回数を増加させると処理量が増大する。更に、認証者側に比較して処理能力の小さい、被認証者側の処理負担が大きいという問題点がある。

【００１１】これらの問題点を解決する方法CINONは、被認証者（ユーザ）が認証者（ホスト）に対して、前回に正当性の検証を終え登録されている被認証データのもとのデータ、次々回に認証に用いる被認証データ、前回送信済みで次回の認証に用いる被認証データの正当性検証データの３つのデータを認証毎に送信することで、認証情報を安全に更新しながら次々と連鎖的に認証を行うことのできる方法である。

【００１２】以下に、CINONの認証手順を説明する。まず、以降の説明に用いる記法を示す。
＜記法＞共通鍵暗号アルゴリズムＥによる一方向性変換をC=E(P, K)で表す、Ｃは一方向性変換データ、Ｐは平文、Ｋは共通鍵である。

【００１３】Ｓを、被認証者の秘密情報、即ち、パスワードとする。ｎは０以上の整数であり、認証回数を示す。Ａを被認証者の識別子、即ち、例えばメールアカウント（被認証者への情報が蓄積される部分）などのユーザＩＤとする。Ｎｎを、認証回数ｎに対応して発生する乱数とする。

11

【００１４】M_nを認証子とする。(+)はビット毎の排他的論理和を表す。$V_n = E(A, S(+)N_n)$とするとき、$W_n = E(A, V_n)$とする。即ち、W_nは、$S(+)N_n$に２度一方向性変換を施したデータであり、W_nから、S，N_nあるいはV_nを逆算することの困難さは、共通鍵暗号アルゴリズムの強さに依存している。

【００１５】＜CINONの認証手順（図１参照）＞

--初期登録処理--

ステップＳ０：被認証者（ユーザ）は初期登録処理を認証者の装置（ホスト装置）で行う。まず、n=0とし、ユーザはユーザ端末で乱数N_0，N_1を生成し、被認証者識別子Ａとパスワードｓを設定する。ユーザはパスワードｓを覚えておき、乱数N_0，N_1を自分のＩＣカード等の媒体に保存しておく。

【００１６】次に、以下の手順：

$V_0 = E(A, S(+)N_0)$

$W_0 = E(A, V_0)$

$V_1 = E(A, S(+)N_1)$

$W_1 = E(A, V_1)$

$M_0 = E(W_1, V_0)$

$n \leftarrow n+1$

でW_0，W_1，M_0を算出し、ユーザ識別子Ａと対応させて認証回数ｎと共に認証側装置（ホスト装置）に登録しておく。W_0は次回の認証データ、W_1は次々回の認証データ、M_0はW_1の正当性検証データである。

--認証処理およびコンテンツデータのやりとり--

初期登録処理（n＝0）終了後、第ｎ回目（n=1,2,…）の認証処理は以下の通りである。なお、この時点で、認証者側には、被認証者の識別子Ａに対応してW_{n-1}，W_n，M_{n-1}，ｎが登録されている。被認証者からのサービス起動要求を受信すると、登録してあるｎを返信する。

【００１７】ステップＳ１：ユーザは、まず、認証者に対してユーザ識別子Ａとサービス要求を送り、サービス起動要求を行う。

ステップＳ２：次に、ホスト装置はユーザ識別子Ａに対応して登録されているｎの値をユーザに送る。

ステップＳ３：ユーザは認証者よりｎの値を受け取り、ＩＣカードから乱数N_{n-1}，N_nを読みだし、新しく乱数N_{n+1}を発生させ、以下の手順：

$V_{n-1} = E(A, S(+)N_{n-1})$

$V_n = E(A, S(+)N_n)$

$V_{n+1} = E(A, S(+)N_{n+1})$

$W_{n+1} = E(A, V_{n+1})$

$M_n = E(W_{n+1}, V_n)$

でV_{n-1}，W_{n+1}，M_nを算出する。

【００１８】ステップＳ５：ユーザはこれらのデータを認証者に送付する。V_{n-1}は、認証者側において、前回に正当性の確認を終え、今回の認証に用いるデータW_{n-1}のもととなったと推定されるデータである。W_{n-1}は、次々回の認証に用いるデータである。また、M_nは、次々回の認証に用いるデータW_{n+1}の正当性検証を次回に検証するためのデータである。

12

【００１９】ステップＳ６：また、ユーザはＩＣカードの乱数N_{n-1}，N_nをN_n，N_{n+1}に書き換える。

ステップＳ７：次に、ホスト装置は被認証者側より送付されてくるV_{n-1}，W_{n+1}，M_nにより、以下の認証処理を行う。

W_{n-1}と$E(A, V_{n-1})$を比較し、一致した場合、被認証者を正当とする。一致しない場合、その被認証者を不当とし、処理を終了する。

【００２０】被認証者を正当とした場合、更に、M_{n-1}と$E(W_n, V_{n-1})$を比較し、一致した場合、W_nを正当とする。一致しない場合、ユーザを不当とし処理を終了する。この２つの検証で共に被認証者を正当とした場合、W_{n-1}，W_n，M_{n-1}は全て正当であると認証し、ステップＳ８でコンテンツデータＴをユーザに送付する。また、ステップＳ９で現在登録してあるデータに換えて、W_n，W_{n+1}，M_nを新たに登録する。また、ｎをインクリメント（＋１）する。

【００２１】このように、CINON では、ユーザが認証者の認証を得るためには、前回生成した２つの乱数N_{n-1}，N_nを使用する必要がある。そのため、ユーザが出先の端末から認証者の認証を得る場合には、ユーザはそれらの乱数N_{n-1}，N_nを記憶した例えばＩＣカードの様な記憶媒体を携帯し、出先の端末で使用しなければならない。また、端末は、乱数を発生する機能及びＩＣカードを読み書きする機能を必要とする。一方、インタネットにおいては、テレビセットやワードプロセッサ、更に携帯端末などにインタネット接続機能を付加したインタネット家電と呼ばれる製品が市場投入されようとしている（参考文献：荒川、鎌田：“インタネット家電がもたらす情報ネットワーク革命，”信学技報、OFS96-1，pp.1-6(1996.5)）。

【００２２】このようなインタネット家電が普及してくることに伴い、認証処理を有した情報の送受信に対する需要が増大してくるものと思われるが、インタネット家電は、コストを最重視しているため、上述の乱数N_{n-1}，N_nを発生したり、それらをＩＣカード等の記憶媒体へ読み書きする機構を有していない場合がほとんどである。また、処理プログラムの格納領域も限られるため、このような認証処理をできるだけ簡易で小さいプログラムサイズで実現することが望まれる。

【００２３】

【発明が解決しようとする課題】この発明の目的は、セキュリティが十分でないネットワーク上の被認証者と認証者間の情報送受信において、被認証者側にＩＣカード等の記憶媒体の読み書きを行う機構を必要とせず、かつユーザ認証処理を小さいプログラムサイズで行うことができる安全な情報送受信制御方法と装置、及びその方法を記録した記録媒体を提供することにある。

13

【００２４】

【課題を解決するための手段】この発明の第１の観点によれば、ネットワーク上でユーザが利用するユーザ端末装置と、認証者の認証者装置との間で認証処理を行うための情報送受信制御方法であり以下のステップを含む：

(a) 初期登録手順として、上記ユーザが、自分の識別子Ａと、秘密に保持しているパスワードＳから、次回認証データW_0、次々回認証データW_1、次々回認証データW_iの正当性検証データM_0の３つを算出し、認証回数ｎの初期値n=1 と共に上記認証者装置に上記識別子Ａと対応して登録し、(b) 次に、ｎを正の整数とすると、第ｎ回目の認証において、上記認証者装置は、上記ユーザ端末装置からサービス起動要求と上記ユーザの識別子Ａの通知を受けて、そのユーザの認証回数ｎを読みだし、そのユーザ端末装置へ通知し、(c) 上記ユーザ端末装置では、上記ユーザの識別子Ａ、送られてきた上記認証回数ｎ及び秘密に保持しているパスワードＳを用いて、今回の認証されるべきデータV_{n-1}、次々回の認証に用いられるデータW_{n+1}、その次々回認証データW_{n+1}の正当性を検証するためのデータM_nを算出し、送信したいコンテンツデータがある場合には、そのデータと共に上記認証者装置に通知し、(d) 上記認証者装置では、上記ユーザの識別子Ａと上記ステップ(c) で送付されてきた今回の認証されるべきデータV_{n-1}とから算出したデータW_{n-1}を、登録されている認証データW_{n-1}と比較し、かつ登録されている次回認証データW_nと、上記今回の被認証データV_{n-1}とから計算した正当性検証データM_{n-1}を、登録されている正当性検証データM_{n-1}と比較し、(e) 上記ステップ(d) の比較の結果、一致した場合、上記認証者装置では、そのユーザを正当とし、上記ユーザが要求したサービスの情報の送受信を行うとともに、前回受けた次回認証データW_nと、今回送付されてきた次々回認証データW_{n+1}、と次々回認証データW_{n+1}の正当性検証データM_nを、前回登録したW_{n-1}, W_n, M_{n-1}と置き換えて登録し、認証回数ｎをインクリメントし、(f) 上記ステップ(d) の比較の結果、一致しない場合、そのユーザを不当とし以降の情報送受信を拒否し、前回登録したW_{n-1}, W_n, M_n及びｎをそのまま保持する。

【００２５】この発明の第２の観点によれば、インタネットにユーザ端末装置と中継サーバがそれぞれ接続されており、そのインタネットに接続されたイントラネットに認証者装置が接続されており、上記ユーザ端末装置と上記認証者装置との間の情報送受信を、上記中継サーバを介して行うシステムにおいて、上記ユーザと認証者との間で認証処理を行うための情報送受信制御方法であり、以下のステップを含む：

(a) 上記ユーザの識別子Ａと、秘密に保持しているパスワードＳから、次回認証データW_0、次々回認証データW_1、その次々回認証データW_iの正当性検証データM_0の３つを算出し、上記認証者装置に上記識別子Ａと対応して登録し、上記認証回数ｎの初期値n=1 を上記認証者装置と上記中継サーバにそれぞれ上記識別子Ａと対応させて保持し、(b) ｎを正の整数とすると、第ｎ回目の認証において、上記中継サーバは上記ユーザ端末装置からサービス要求と識別子Ａを受けると、対応する認証回数ｎを読みだし、上記ユーザ端末装置に送り、(c) 上記ユーザ端末装置では、上記ユーザの識別子Ａ、送られてきた上記認証回数ｎ及び秘密に保持しているパスワードＳを用いて、今回の認証されるべきデータV_{n-1}、次々回の認証データW_{n+1}、その次々回認証データW_{n+1}の正当性検証データM_nを算出し、送信したいコンテンツデータがある場合には、そのデータと共に上記中継サーバを介して上記認証者装置に送り、その後上記中継サーバとの接続を一旦切断し、(d) 上記認証者装置では、上記ユーザの識別子Ａと上記ステップ(c) で送付されてきた今回の被認証データV_{n-1}とから算出した今回の認証データW_{n-1}を、登録されている認証データW_{n-1}と比較し、かつ登録されている次回認証データW_nと、上記今回の被認証データV_{n-1}とから計算した正当性検証データM_{n-1}を、登録されている正当性検証データM_{n-1}と比較し、(e) 上記ステップ(d) の比較の結果、一致した場合、上記認証者装置では、そのユーザを正当とし、上記ユーザが要求したサービスの情報を上記中継サーバに転送して、そこに保管し、或いは、送信したいコンテンツ情報がある場合には、認証されたユーザの資格でその情報の送信を行い、送信を完了したことを示す確認情報を中継サーバに送信し、(f) 上記認証者装置は更に、前回受けた次回認証データW_nと、今回送付されてきた次々回認証データW_{n+1}とその次々回認証データの正当性検証データM_nを、前回登録したW_{n-1}, W_n, M_{n-1}と置き換えて登録し、認証回数ｎをインクリメントし、上記ステップ(d) の比較の結果、一致しない場合、そのユーザを不当とし以降の情報送受信を拒否し、前回登録したW_{n-1}, W_n, M_n及びｎをそのまま保持し、(g) 上記中継サーバは、上記サービス情報或いは上記送信確認情報を受け取った後、上記認証回数ｎをインクリメントし、(h) 上記ユーザは、上記中継サーバとの接続を切断してから一定時間が経過した後の任意の時間に上記中継サーバに再度接続し、上記中継サーバとの間で上記サービス情報に対する上記ユーザの正当性を検証する認証処理を行い、上記サービス情報を受信し、ここで、上記ユーザ端末装置と上記中継サーバ間の情報のやりとりは高速通信プロトコルを使って行い、上記中継サーバと上記認証者装置間の情報のやりとりは電子メールプロトコルを使って行う。

【００２６】この発明の第３の観点によれば、ユーザ端末装置と、サービスプロバイダと、認証者装置（課金管理センタ）とがインタネットに接続されており、ユーザがインタネット上でサービスプロバイダからサービスを受ける場合に、ユーザが課金管理センタとの間で認証処理を行うための情報送受信制御方法であり、以下のステ

14

15

ップを含む：

(a) 初期登録手順として、上記ユーザのアカウントＡと、パスワードＳから次回認証データW_0、次々回認証データW_1、その次々回認証データの正当性検証データM_0の３つを計算し、認証回数初期値n=1 と、金額Ｘと共に上記アカウントＡと対応して登録し、(b) ユーザは上記サービスプロバイダに所望のサービスを要求するサービス要求信号とアカウントＡを送り、(c) 上記サービスプロバイダは受信した上記アカウントＡを上記課金管理センタに転送し、(d) 上記課金管理センタは上記アカウントＡに対応する認証回数ｎを読み出し、上記サービスプロバイダに送り、(e) 上記サービスプロバイダは受信した認証回数ｎを認証手順のAppletプログラムと共にユーザ端末装置に送り、(f) 上記ユーザは上記認証手順に従って認証用データV_{n-1}, W_{n-1}, M_nを計算し、上記アカウントＡと共に上記サービスプロバイダに送り、(g) 上記サービスプロバイダはデータV_{n-1}, W_{n-1}, M_nと共に上記サービスプロバイダのアカウントA_rと、上記サービスに対する金額ｘを上記課金管理センタに送り、(h) 上記課金管理センタは上記サービス金額ｘが上記アカウントＡに対応して登録されている残額Ｘ以下であることを確認し、受信したデータV_{n-1}と登録されている次回認証データW_nを検証し、両方とも正しければ認証確認信号OKを上記サービスプロバイダに送ると共に、データW_n, W_{n+1}, M_nに更新し、認証回数ｎをインクリメントし、上記アカウントＡの残額ＸをX-x で更新し、上記プロバイダのアカウントA_rの残額XPをX_r+xで更新し、(i) 上記サービスプロバイダは、上記確認信号OKを受けると上記ユーザに上記指定されたサービスを提供する。

【００２７】この発明の第４の観点によれば、ネットワーク上でユーザの正当性を認証するための情報送受信制御を行う認証者装置であり、以下を含む：ｎを正の整数とすると、次回認証データW_{n-1}、次々回認証データW_n、次々回認証データW_nの正当性検証データM_{n-1}を認証回数ｎと共に上記識別子Ａと対応して第n-1 回目の認証時に登録した登録データ記憶手段と、第ｎ回目の認証において、上記ユーザの端末装置からサービス起動要求と上記ユーザの識別子Ａの通知を受けて、そのユーザの認証回数ｎを上記登録データ記憶手段から読みだし、そのユーザ端末装置へ通知する認証回数送出手段と、上記ユーザ端末装置から送られてきた今回の被認証データV_{n-1}、次々回の認証データW_{n+1}、次々回認証データW_{n+1}の正当性検証データM_nを受信する受信手段と、上記ユーザの識別子Ａと上記受信した今回の被認証データV_{n-1}とから算出した今回の認証データW_{n-1}を、上記登録データ記憶手段に登録されている認証データW_{n-1}と比較し、かつ登録されている次回認証データW_nと、上記今回の被認証データV_{n-1}とから計算した正当性検証データM_{n-1}を、登録されている正当性検証データM_{n-1}と比較する認証手段と、及び上記認証手段による比較の結果、一致した場合、そのユーザを正当とし、登録されている次回認証データW_nと、今回受信した次々回認証データW_{n+1}と、及び今回受信した次々回認証データW_{n+1}の正当性検証データM_nとを、上記登録データ記憶手段に登録されているW_{n-1}, W_n, M_{n-1}と置き換えて登録し、認証回数ｎをインクリメントする登録更新手段。

16

【００２８】この発明の第５の観点によれば、ネットワーク上でユーザの正当性を認証する認証者側の認証手順を記録した記録媒体であり、上記認証手順は以下を含む：

(a) ユーザの識別子Ａとパスワードｓを使って次の一方向性関数

$V_0 = E(A, S)$

$W_0 = E(A, V_0)$

$V_1 = E(A, S(+)1)$

$W_1 = E(A, V_1)$

$M_0 = E(W_1, V_0)$

によりデータ初期値W_0, W_1, M_0を算出して登録し、(b) ｎを正の整数とすると、第ｎ回目の認証において、上記ユーザの端末装置からサービス起動要求と上記ユーザの識別子Ａの通知を受けて、そのユーザの認証回数ｎを上記登録データ記憶手段から読みだし、そのユーザ端末装置へ送信し、(c) 上記ユーザ端末装置から送られてきた今回の被認証データV_{n-1}、次々回の認証データW_{n+1}、次々回認証データW_{n+1}の正当性検証データM_nを受信し、(d) 上記ユーザの識別子Ａと上記受信した今回の被認証データV_{n-1}とから一方向性関数$W_{n-1}=E(A,V_{n-1})$により今回の認証データW_{n-1}を算出し、上記登録データ記憶手段に登録されている認証データW_{n-1}と比較し、かつ登録されている次回認証データW_nと、上記今回の被認証データV_{n-1}とから一方向性関数$M_{n-1}=E(W_n, V_{n-1})$により正当性検証データM_{n-1}を算出し、登録されている正当性検証データM_{n-1}と比較し、(e) ２つの比較結果が同時に一致であった場合、そのユーザを正当とし、登録されている次回認証データW_nと、今回受信した次々回認証データW_{n+1}と、及び今回受信した次々回認証データの正当性検証データM_nとを、上記登録データ記憶手段に登録されているW_{n-1}, W_n, M_{n-1}と置き換えて登録し、認証回数ｎをインクリメントする。

【００２９】この発明の第６の観点によれば、ネットワーク上で認証者からユーザに対する認証を得るユーザ側の手順を記録した記録媒体であり、上記手順は以下を含む：

(a) サービス要求とユーザの識別子Ａを上記認証者装置に送信し、(b) ｎを正の整数とすると、上記認証者装置から認証回数ｎを受信し、(c) 上記ユーザの識別子Ａ、受信した上記認証回数ｎ及び秘密に保持しているパスワードＳを用いて、今回の被認証データV_{n-1}、次々回の認証データW_{n+1}、次々回認証データW_{n+1}の正当性検証データM_nを次の一方向性関数

17

$V_{n-1} = E(A, S(+)(n-1))$

$V_n = E(A, S(+)n)$

$V_{n+1} = E(A, S(+)(n+1))$

$W_{n+1} = E(A, V_{n+1})$

$M_n = E(W_{n+1}, V_n)$

により算出し、上記認証者装置に送信する。

【００３０】この発明は、認証手順において、従来技術において被認証データ生成時に用いていた乱数に代えて、認証回数を用いるようにしたことを最も主要な特徴とする。この発明においては、被認証データの生成に用いる一方向性変換にＤＥＳやＦＥＡＬなどの共通鍵暗号方法を用いる。これらの暗号方法は、先述の通り、平文や共通秘密鍵の入力が１ビット変化しただけでも、その入力の痕跡をまったくとどめない出力を得ることができる。一方向性変換のこの特徴に着目し、従来技術が、乱数と秘密に保持しているパスワードの２つを鍵にして被認証データを生成していたのに対して、一方を定数である認証回数とすることで、従来と同等の強度を持つ認証機能を有し、かつ、この発明の目的である乱数を記憶するためのＩＣカード及びそれに対する読み書き機構、乱数発生機構を必要としない簡易な情報送受信を実現することができる。つまりこの発明では従来の乱数にかえ認証回数を用いているが、安全性は用いる一方向性関数、つまり共通暗号方法の強度に依存し、認証回数に変更した影響はない。

【００３１】

【発明の実施の形態】

実施例１

図２は、この発明の第１の実施例の概要を説明する図である。インタネットの普及により、電子メールがインタネットを介したコミュニケーションの手段として、特にビジネスの分野において幅広く用いられるようになってきた。これに伴い、ビジネスユーザを中心に、出先からメールメッセージを送受したいといった要求が高まってきている。

【００３２】パソコン通信の場合は、電話網を用いて共通のセンタへアクセスし、メッセージの読み出しや書き込みを行うため、例えば出先端末からでも、ＩＳＤＮ公衆電話網にモデム機能を有した携帯型のパソコンを接続するなどして、メッセージの送受信を行うことができる。これに対して、インタネットでは、電話網におけるパソコン通信と同じように、メールサーバをセンタと考えて電話網経由でアクセスすることが可能であるが、セキュリティ上の問題から、あらかじめ登録してある電話番号にコールバックさせたり、モデム経由でのアクセスを制限している場合が多い。また、一般にモデムアクセス用に用意している電話回線の数は少なく、回線が話中でつながらない場合が多いなど、場所が定まらない出先からのアクセスは困難である場合が多い。

【００３３】また、インタネット本来の特徴であるＩＰアドレスレベルでの接続（レイヤ３での接続）を考えた場合、不定な出先、即ち、不特定のＩＰアドレスからの接続要求は、メールサーバ１３のある内部ネットワーク１２への入口に設けてあるファイアウォール１２Ｆによって拒否される。つまり、電子メール（レイヤ７）で使われるプロトコル（即ちSMTP：Simple Mail Transfer Protocol)はファイアウォールを通過することができるように決められている。この実施例では、出先から電話網を使わず、ファイアウォールを回避して、インタネット経由で安全に自分宛のメールメッセージを取り出したり送信したりすることのできる公衆電子メール転送サービスにおけるメールサーバの、ユーザに対する認証にこの発明を適用した場合を説明する。

【００３４】公衆電子メール転送サービスが有するべき一般要求およびセキュリティ上の要件について述べる。まず、この明細書で扱う公衆電子メール転送サービスが有する一般要件は以下の通りである。

(1) このサービスのユーザ（利用者）は、インタネット上のあるメールサーバに固有のメールアカウントを有している。

【００３５】(2) ユーザは、ユーザ固有のメールアカウントがある環境において常駐されたこのサービスのアプリケーションを、また、出先の環境において、このサービスのアプリケーションプログラムを用いることができる。

(3) ユーザは、出先において、テンポラリなアカウントを用い、本来のアカウント宛に届いている電子メールを受信できる。同様に、テンポラリなアカウントを用い、本来のアカウントからのメール送信ができる。ここで、テンポラリなアカウントとは、例えば公衆に使用が提供されている、インタネットに接続された端末や、他ユーザのアカウントなどである。

【００３６】図２の例ではインタネット１１に企業内のＬＡＮのような内部ネットワーク１２が接続され、その内部ネットワーク１２に、ユーザＵ１のメールアカウントがあるホスト装置（サーバー装置：認証者装置）１３が接続され、ユーザＵ１はホスト装置１３の接続された内部ネットワーク１２を通じて、ホスト装置１３の自己のメールアカウント宛に届いている電子メールを受信できる。

【００３７】ユーザＵ１が移動して、内部ネットワーク１２の外部へ移動した状態で、その移動先の、インタネット１１に加入している例えばパソコン１４にユーザＵ１の識別子Ａとパスワードｓを入力し、ユーザＵ１の識別子Ａを電子メールとしてインタネット１１、内部ネットワーク１２を介して、ユーザＵ１のメールアカウントがあるホスト装置（被認証者装置）１３へ送り、ホスト装置１３との間でこの発明による認証手順を実施すれば、ユーザＵ１のメールアカウント宛に届いている電子メールを受信することができる。つまりパソコン１４が

19

インタネット１１に加入しているアカウントを一時的に借りて、本来のアカウントＡに宛ている電子メールを受信できる。

【００３８】更にインタネット１１と接続された他の内部ネットワーク１５に収容されている端末１６にユーザＵ１は自己の識別子Ａ、パスワードＳを入力し、識別子Ａを電子メールとして内部ネットワーク１５－インタネット１１－内部ネットワーク１２を介してホスト装置１３に入力して、この発明による認証手順を実施することにより、その自己メールアカウントに届いている電子メールを取出すことができる。

【００３９】しかし、別のユーザＵ２が端末１７を通じて、ユーザＵ１になりすまして、そのメールアカウントに届いている情報を取出そうとしても、即ち、ユーザＵ１の識別子Ａを使ってホスト装置１３にアクセスしたとしても、ユーザＵ１のパスワードＳを知らないため、認証手順を正しく実行できず、ホスト装置１３のユーザＵ１のメールアカウントに届いた情報を取出すことはできない。

【００４０】上述では電子メールの読出し（受信）について述べたが、電子メールの書込み（送信）も同様に行うことができる。公衆電子メール転送サービスが有するべき一般的要件により、以上のように電子メールの受信、送信が可能であるが、この公衆電子メール転送サービスが有するべきセキュリティ上の要件は以下の通りである。

【００４１】(1) ユーザは、記憶しているパスワード等が認証されることによって、メールサーバのある環境に設定されたファイアウォールを回避でき、出先において、安全にメール送受信サービスの提供を受けることができる。これに対して、資格のない者のメール送受信は阻止される。

(2) 回線上およびメールサーバ内データベースから、ユーザのパスワードを盗取できない。

【００４２】(3) 認証のための処理負担が、ユーザのメールアカウントがある環境および出先の環境の双方において少ない。特に、インタネット上を流れるデータは、簡単に盗聴されるため、パスワードが回線上をそのまま流れるような手順は用いられない。第１実施例はこのような条件(1), (2), (3) を満たす電子メール転送サービスにおける認証手順にこの発明を適用した場合である。従って、ユーザとメールサーバ間の通信は電子メールのプロトコルを使って行う。なお、以下の説明に用いる記法は、従来技術の説明に用いたものと同じである。

＜初期登録処理（図３）＞ステップＳ０：初期登録処理として、ユーザは識別子（メールアカウント）Ａと認証回数初期値n=0 をメールサーバ１３に直接設定する。

【００４３】次に、ユーザはメールサーバ１３において以下の手順：

$$V_0 = E(A, S) \quad (1a)$$

20

$$W_0 = E(A, V_0) \quad (1b)$$

$$V_1 = E(A, S(+)1) \quad (1c)$$

$$W_1 = E(A, V_1) \quad (1d)$$

$$M_0 = E(W_1, V_0) \quad (1e)$$

でW_0, W_1, M_0を算出し、ユーザのメールアカウントＡに対応させてメールサーバ（認証者装置）内に登録しておく。更に、ｎを１にインクリメントし、識別子Ａに対応して登録しておく。W_0は次回の認証データ、W_1は次々回の認証データ、M_0はW_1の正当性検証データをそれぞれ表している。

＜認証処理およびメールメッセージのやりとり＞図３は初期登録処理終了後、第ｎ回目（n=1,2,…）の認証手順を以下に示す。

【００４４】ステップＳ１：出先にいるユーザは、出先の端末（図２における端末１４）を使ってまず自分のメールアカウントがあるメールサーバに対して、特定のヘッダ（SMTP）を有する電子メールでメールサービス要求（以下、メール要求と呼ぶ）を送出すると共にメールアカウントＡを通知する。メール要求は、メール送信、メール受信、ファイル転送送信、ファイル転送受信のいずれかを指定するものである。

【００４５】ステップＳ２：メールサーバは出先にいるユーザからのサービス起動要求メールを受信すると、メールアカウントＡに対応して登録してある認証回数ｎを、メールで返信する。この時点で、ホスト側には、既に、W_{n-1}, W_n, M_{n-1}が登録されている。

ステップＳ３：ユーザはメールサーバからメールで、ｎの値を受け取り、以下の手順：

$$V_{n-1} = E(A, S(+)(n-1)) \quad (2a)$$

$$V_n = E(A, S(+)n) \quad (2b)$$

$$V_{n+1} = E(A, S(+)(n+1)) \quad (2c)$$

$$W_{n+1} = E(A, V_{n+1}) \quad (2d)$$

$$M_n = E(W_{n+1}, V_n) \quad (2e)$$

でV_{n-1}, W_{n+1}, M_nを算出し、更に、ステップＳ４でメールにより、これらのデータ、および送信したいメールのある場合にはその情報を、自分のメールサーバに送付する。V_{n-1}はメールサーバ側において、前回に正当性の確認を終え、今回の認証に用いる、一方向性関数の変換により得られるデータ（一方向変換データと呼ぶ）W_{n-1}の元となったと推定されるデータである。W_{n+1}は、次々回の認証に用いる一方向変換データである。また、M_nは次々回の認証に用いる一方向変換データW_{n+1}の正当性を次回に確認するための認証データである。

【００４６】ステップＳ５：メールサーバは、ユーザ側より受信したV_{n-1}, W_{n+1}, M_nにより、以下の認証処理を行う。登録されているW_{n-1}と、受信したV_{n-1}を使って一方向性関数Ｅにより計算した$E(A, V_{n-1})$とを比較し、一致した場合、ユーザを正当とする。一致しない場合、そのユーザを不当とし、処理を終了する。

【００４７】ユーザを正当とした場合、更に、M_{n-1}とＥ

21

(W_n, V_{n-1})を比較し、一致した場合、W_nを正当とする。一致しない場合、W_nを不当とし処理を終了する。正当とされたこのW_nは次回(n+1)の認証においてデータW_{n-1}として受信V_{n-1}の正当性（ユーザの正当性）の判定に使用されることになる。これらの認証処理によりユーザ及びW_nが正当と判定された場合、ステップＳ６でユーザ宛の新着メールがあれば、それをユーザにメールで送付する。また、ユーザからの送信メールがある場合には、ユーザの本来のアカウントでそのメールを送信する。

【００４８】更に、ステップＳ７で現在登録してあるデータW_{n-1}, W_n, M_{n-1}に換えて、W_n, W_{n+1}, M_nを新たに登録する。また、ｎをインクリメントする。図４は上述の第１実施例で使用されるユーザ端末の機能ブロック図を示す。ユーザ端末は、入力部２１と、制御部２２と、受信部２３と、送信部２４と、認証用データ生成部３０と、メモリ２５と、出力部２６とから構成されている。入力部２１にはユーザが識別子Ａ、パスワードＳ、接続先アドレス（メールサーバアドレス）、メール要求、等の情報を入力する。制御部２２はメールサーバにメール要求及び識別子Ａを送信部２４から送信すると共に、認証用データ生成部３０に識別子Ａとパスワードを設定する。受信部２３により受信されたメールサーバからの認証回数ｎは減算器３１ａで１が減算され、その出力n-1が排他的論理和部３２ａでパスワードＳと排他的論理和が取られる。排他的論理和部３２ａの出力は識別子Ａと共に一方向性関数部３３ａに与えられ、式(2a)によりデータV_{n-1}が計算される。受信部２３からの認証回数ｎは加算部３１ｃにも与えられ、１が加算され、その加算結果n+1が排他的論理和部３２ｃでパスワードＳと排他的論理和が取られる。排他的論理和部３２ｃの出力は識別子Ａと共に一方向性関数部３３ｃに与えられ、式(2c)によりデータV_{n+1}が計算される。データV_{n+1}は識別子Ａと共に更に一方向性関数部３４ｄに与えられ、式(2d)によりデータW_{n+1}が計算される。認証回数ｎは更に排他的論理和部３２ｂにも与えられ、パスワードＳとの排他的論理和が取られる。その出力は識別子Ａと共に一方向性関数部３３ｂに与えられ、式(2b)によりデータV_nが計算され、更に、データV_nと一方向性関数部３４ｄの出力W_{n+1}が一方向性関数部３４ｅに与えられ、式(2e)によりデータM_nが計算される。この様にして計算された認証用データV_{n-1}, W_{n+1}, M_nはレジスタ３５に一時的に保持され、送信部２４からメールサーバに送出される。

【００４９】メールサーバ１３による認証後、メールサーバ１３から受信したメールメッセージはメモリ２５に一時保持され、必要に応じてプリンタ或いは表示器などの出力部２６に出力する。図４に示したユーザ端末の機能構成における制御部２２、メモリ２５、認証用データ生成部３０は実際にはコンピュータのソフトウエアとして実現される。即ち、端末コンピュータは図３における

22

ユーザ側処理手順を実行するプログラムが記録された記録媒体を有しており、そのプログラムに従ってユーザ側の認証処理手順を実行する。

【００５０】図５は、図２及び３の実施例におけるメールサーバ１３の機能ブロック図を示す。メールサーバ１３は入力部４１、初期登録部５０、認証部６０、制御部４４、認証回数歩進部４５、メモリ４３から構成されている。初期登録部５０は、初期登録時（ステップＳ０）にユーザにより入力部４１から入力された識別子（メールアカウント）ＡとパスワードＳとから式(1a)によりV_0を計算する一方向性関数部５１と、そのV_0と識別子Ａから式(1b)によりW_0を計算する一方向性関数部５２と、式(1c)中のパスワードＳと１との排他的論理和を計算する排他的論理和部５３と、その排他的論理和出力と識別子Ａとから式(1c)によりV_1を計算する一方向性関数部５４と、V_1とＡとから式(1d)によりW_1を計算する一方向性関数部５５と、W_1とV_0とから式(1e)によりM_0を計算する一方向性関数部５６とから構成されている。

【００５１】制御部４４はこれらの計算した初期値W_0, W_1, M_0を識別子Ａと対応させてメモリ４３に登録する。また、歩進部４５により認証回数ｎを１インクリメントして識別子Ａに対応させてメモリ４３に記憶する。ユーザのｎ回目の認証において、レジスタ４６には、メモリ４３から読みだした認証回数ｎを歩進部４５により＋１した歩進結果n+1と、ユーザから受信した認証用データW_{n-1}, M_nと、及びメモリ４３から読み出したデータW_nとが一時的に保持されている。認証部６０は、識別子Ａを有するユーザから受信した識別子ＡとデータV_{n-1}とから$E(A, V_{n-1})$を計算する一方向性関数部６１と、計算したそのデータW_{n-1}とメモリ４３から識別子Ａと対応して読みだしたデータW_nとを比較し、一致(OK)、不一致(NG)の比較結果OK/NGを出力する比較部６２と、受信したデータV_{n-1}とメモリ４３から読みだしたデータW_nとからデータM_{n-1}を計算する一方向性関数部６３と、そのデータM_{n-1}とメモリ４３から読みだしたデータM_{n-1}を比較し、一致、不一致の比較結果を出力する比較部６４とから成る。制御部４４は、比較部６２及び６４の出力が両方ともOKであれば、メモリ４３に識別子Ａと対応して保管されているユーザ宛のメールメッセージを読みだし、送受信部４２からユーザに送出すると共に、レジスタ４６に保持されているデータｎ, W_n, W_{n+1}, M_{n-1}でメモリ４３の識別子Ａに対応して登録されているデータW_{n-1}, W_n, M_{n-1}を書き換える。

【００５２】図５に示したメールサーバ装置の機能構成におけるメモリ４３、制御部４４、歩進部４５、レジスタ４６、初期登録部５０及び認証部６０はコンピュータのソフトウエアとして実現される。即ち、メールサーバコンピュータは図３におけるメールサーバ側処理手順を実行するプログラムが記録された記録媒体を有してお

23

り、そのプログラムに従ってサーバ側の認証処理を実行する。

【００５３】上述の第１実施例において、一方向性変換をFEAL暗号方式で実現した場合、被認証者側の認証処理を0.6KByte程度（うち、FEALが0.4KByte）のプログラムで記述することができる。このように、この発明ではユーザは図１で示したCINON と同様に、認証処理において自分のパスワードＳをメールサーバに送信しないので、インタネットを通した認証処理を安全に行うことができる。しかも、CINON で必要とされた乱数を使用しないので、乱数を記憶しておくためのＩＣカードの様な記録媒体を必要とせず、また乱数生成機能、及びＩＣカードへの読み書き機能を必要としない。また、乱数を使用しないので、それだけ認証処理のデータサイズが小さくてよい。従って、ホスト装置においては認証処理時間が短い。これは、この発明が処理能力の低いホスト装置とでも使用可能であることを示している。

実施例２

上述の第１実施例では、この発明の認証方法をSMTP通信を使った電子メールでのユーザとメールサーバ間の認証手順に適用した場合を説明したが、ユーザがインタネット上でホストサーバによる各種サービスをHTTP通信を使って受ける場合における、ユーザとホスト間の認証手順にこの発明を適用してもよい。その場合の実施例を次ぎに説明するが、ここでは更に、ユーザ側の認証手順（プログラム）をホスト側からアプレットとして受信し、それを使う場合に付いて説明する。

【００５４】インタネット利用の高度化、多様化に対応して端末には各種プログラムを内蔵することなく、その端末の処理要求に応じて、その処理手順（プログラム）をその都度、その端末は相手（サーバ）から通信を介して送り込まれ、その送り込まれた処理手順をその端末が実行する方法が普及しようとしている。これは、インタネットにおいて、ユーザからの情報送受信要求があった時に、サーバ側が要求された処理手順を予め決められた言語、例えばJavaで記述された特定の通信単位、例えばAppletに埋め込んだものをユーザに送り込み、ユーザ側でその処理手順（プログラム）にもとづく処理が実行されるというもので、従来のＯＳ（オペレーティングシステム）の概念を根底から変えてしまう画期的な方法である。今後、このような方法を用いる情報送受信が普及してくることに伴い、ユーザの認証機能がますます重要になってくる。第２の実施例は、この発明の認証方法をこのような手法環境へ適用するものである。

【００５５】なお、以下の説明に用いる記法は、これまでの説明に用いたものと同じである。以下の動作説明において、通信はHTTPで行われる。

＜初期登録処理（図６）＞ステップＳ１：ユーザ（被認証者）は、サーバ（認証者装置）に対して、初期登録要求を識別子（アカウント）Ａと共に送る。

24

【００５６】ステップＳ２：サーバはこの要求に対応してユーザ識別子Ａを登録する。

ステップＳ３：サーバは更に初期登録処理を記述した通信単位（Applet）をユーザに送付する。

ステップＳ４：この通信単位プログラムを受信したユーザは、ユーザ端末においてそのアプレットプログラムを使ってユーザ識別子Ａ及びパスワードＳを設定する。

【００５７】ステップＳ５：ユーザは更にアプレットプログラムを使って、以下の手順：

$V_0 = E(A, S)$

$W_0 = E(A, V_0)$

$V_1 = E(A, S(+)1)$

$W_1 = E(A, V_1)$

$M_0 = E(W_1, V_0)$

$n \leftarrow n+1$

で、初期データW_0, W_1, M_0を算出する。

【００５８】ステップＳ６：ユーザは識別子Ａと共にサーバ側へ送信する。W_0は次回の認証データ、W_1は次々回の認証データ、M_0はW_1の正当性検証用データである。

ステップＳ７：サーバ側では、受信した識別子Ａと対応させて、認証回数ｎの初期値n=1 及び受信したデータW_0, W_1, M_0を登録する。

＜認証処理および情報のやりとり（図７）＞初期登録処理（図６におけるステップＳ７）の終了後、第ｎ回目（n=1,2,…）の認証手順は以下の通りである。なお、この時点で、ホスト側には、既に、n, W_{n-1}, W_n, M_{n-1}が登録されている。

ステップＳ１：ユーザは、まずサーバに対して、サービス起動の要求を送出すると共にユーザ識別子Ａを通知する。

【００５９】ステップＳ２：サーバは出先にいるユーザからの、サービス起動要求とユーザ識別子Ａを受信すると、認証処理Appletと、識別子Ａに対応して登録されている認証回数ｎとをユーザに返信する。

ステップＳ３：ユーザはサーバ側より、認証処理Appletとｎの値を受け取り、アプレットプログラムに従って以下の手順：

$V_{n-1} = E(A, S(+)(n-1))$

$V_n = E(A, S(+)n)$

$V_{n+1} = E(A, S(+)(n+1))$

$W_{n+1} = E(A, V_{n+1})$

$M_n = E(W_{n+1}, V_n)$

で認証用データV_{n-1}, W_{n+1}, M_nを算出する。

【００６０】ステップＳ４：ユーザは更に、これらのデータV_{n-1}, W_{n+1}, M_n、及び送信したい情報がある場合にはその情報を、サーバに送付する。

ステップＳ５：サーバはユーザ側より送付されてきたデータV_{n-1}, W_{n+1}, M_nにより、以下の認証処理を行う。識別子Ａと対応して登録されているデータW_{n-1}と、受信し

たデータV_{n-1}から計算したE(A, V_{n-1})とを比較し、一致した場合、ユーザを正当とする。一致しない場合、そのユーザを不当とし、処理を終了する。

【００６１】ユーザを正当とした場合、更に、登録されているM_{n-1}とE(W_n, V_{n-1})を比較し、一致した場合、W_nを正当とする。一致しない場合、W_nを不当とし処理を終了する。

ステップＳ６：サーバはユーザ及びW_nの両方を正当と判定した場合、要求された情報送受信サービスの提供を開始する。

【００６２】ステップＳ７：サーバは更に、現在登録してあるデータW_{n-1}, W_n, M_{n-1}に換えて、W_n, W_{n+1}, M_nを識別子Ａに対応して新たに登録する。また、ｎをインクリメントする。この実施例においても、実施例１の場合と同様に、一方向性関数ＥをFEAL暗号方法で実現した場合、認証処理を0.6KByte程度（うち、FEALが0.4KByte）のプログラムで記述することができる。このサイズは、Appletへプログラムを記述した場合、通信への負荷をほとんど生じさせない規模である。

【００６３】実施例１では電子メールへこの発明を適用し、電子メールにより、出先端末の電子メール加入者の環境を一時的に借りてファイアウォールに影響されることなく、自己へのメッセージを受け取ることが可能なことを示し、実施例２においては通信プロトコル（HTTP）によりこの認証処理を行うことを示した。更に、これら両実施例を組み合わせた以下に説明する第３実施例のような形態も可能である。

実施例３

一般にインタネットは混雑していて、情報が円滑に送受信できない場合が多い。実施例１で示したように、ファイアウォールを回避するために認証情報を電子メールプロトコルでやりとりする場合、条件によっては数分間の時間を要する。この間、利用者に待機を強いるのはサービス上好ましくないと考えられる場合、図８に示すように、ユーザ端末１４とメールサーバ１３の間に中継サーバ１８を設ける。メールサーバ１３がファイアウォール１２Ｆの内側、即ちイントラネット１２の内部ネットワークにあるのに対して、この中継サーバ１８は、インタネット１１上にあり、外部に公開しているものとする。また、中継サーバ１８はユーザに対する認証機能を持っているものとする。認証機能は従来提案されているどの様なものでもよいが、以下の説明では、この発明を適用した認証処理を行うものとする。メールサーバ１３には前述した実施例１又は２の場合と同様に予めユーザが識別子Ａに対応させてデータn=1, W_0, W_1, M_0 を初期登録しておく。又、ユーザと中継サーバ間の認証回数をｎ'で表すと、中継サーバにユーザの識別子Ａと対応させてデータn'=1, W_0, W_1, M_0を初期登録しておく。

【００６４】第３実施例においては、インタネットに接続された端末１４とイントラネット１２に接続されたメールサーバ１３との通信は、中継サーバ１８を介して行い、しかも、インタネット１１に接続された端末１４と中継サーバ１８間はHTTPなどの高速転送プロトコルを用いて送受信を行い、中継サーバ１８とメールサーバ１３との間はSMTPのような電子メールプロトコルを使って通信を行う。

【００６５】図９はこの様なシステムにおいて、ユーザが出先のインタネット端末１４からｎ回目にメールサーバ１３に自分宛の電子メールを取りにいく場合の手順を示している。ただし、この時点でメールサーバ１３には識別子Ａに対応してデータn,W_{n-1}, W_n, M_{n-1} が登録されており、中継サーバ１８には識別子Ａに対応してデータn', W_{n-1}, W_n, M_{n-1} が登録されている。

【００６６】ステップＳ１：ユーザはインタネット１１に接続された端末１４からメール要求と、自分の識別子Ａとを中継サーバ１８に送る。

ステップＳ２：中継サーバ１８は受信したメール要求と識別子Ａを電子メールでメールサーバ１３に送る。

ステップＳ３：メールサーバ１３は受信した識別子Ａに対応する認証回数ｎを中継サーバ１８に電子メールで送信し、

ステップＳ４：中継サーバ１８はその認証回数ｎをユーザに転送する。

【００６７】ステップＳ５：ユーザは受信した認証回数ｎを使って図３又は７のステップＳ３と同様の手順により認証用データV_{n-1}, W_{n+1}, M_nを計算し、更に

ステップＳ６：ユーザはそれら認証用データを識別子Ａ及びメール要求と共に中継サーバに送る。メール要求がメール送信の場合は、送信すべきメールメッセージも送る。ここで、ユーザは一旦、中継サーバ１８との接続を切断し、必要に応じて他のタスクを実行する。

【００６８】ステップＳ７：中継サーバ１８は受信した識別子Ａ、メール要求（及び送信すべきメッセージ）、認証用データV_{n-1}, W_{n+1}, M_nを電子メールによりメールサーバ１３に転送する。

ステップＳ８：メールサーバ１３は受信した識別子Ａに対応して登録されているデータW_{n-1}, W_n, M_{n-1}を読みだし、図３又は７のステップＳ５と同様の手順により、受信したV_{n-1}の正当性と次回n+1 の認証に使用するW_nの正当性を認証する。これら２つが正当であると判定されると、

ステップＳ９：メールサーバは識別子Ａに対応するユーザ宛のメールメッセージを中継サーバに転送し、或いは、送信すべきメッセージを送出し、送出確認情報を中継サーバに送る。更に、

ステップＳ１０：メールサーバは登録されているデータW_{n-1}, W_n, M_{n-1}をW_n,W_{n+1}, M_nに書き換えると共に、ｎをインクリメントする。

【００６９】ステップＳ１１：中継サーバは受信した識別子Ａ宛の電子メールメッセージ及び／又は送信確認情

27

報を識別子Ａに対応して保管する。

ステップＳ１２：ユーザは中継サーバとの接続を切断して数分経過した後、任意の時間に中継サーバに識別子Ａとメール要求を送る。

ステップＳ１３：中継サーバは識別子Ａに対応して登録してある認証回数ｎ'を読みだし、ユーザに送る。

【００７０】ステップＳ１４：ユーザは受信したｎ'を使って図３又は７のステップＳ３と同様の手順で認証用データV_{n-1}, W_{n-1}, M_{n} を計算し、

ステップＳ１５：ユーザはそれらを中継サーバに送る。

ステップＳ１６：中継サーバは受信したデータV_{n-1}, W_{n-1}, M_{n} から図３又は７のステップＳ５と同様の手順でV_{n-1} とW_{n} の正当性を認証し、それによってメールを要求しているユーザが正当なユーザであると判定し、

ステップＳ１７：中継サーバは識別子Ａに対応して保管してある電子メールメッセージをユーザに転送する。更に、

$$V_0 = E(A(+)A_u, S)$$
$$W_0 = E(A(+)A_u, V_0)$$
$$V_1 = E(A(+)A_u, S(+)1)$$
$$W_1 = E(A(+)A_u, V_1)$$
$$M_0 = E(W_1, V_0)$$

及び

$$V_{n-1} = E(A(+)A_u, S(+)(n-1))$$
$$V_n = E(A(+)A_u, S(+)n)$$
$$V_{n+1} = E(A(+)A_u, S(+)(n+1))$$
$$W_{n-1} = E(A(+)A_u, V_{n+1})$$
$$M_n = E(W_{n+1}, V_n)$$

のように、識別子Ａの代わりに$A(+)A_u$を使い、メールサーバの認証ステップＳ８において$W_{n-1}=E(A(+)A_u, V_{n-1})$の一致と、$M_{n-1}=E(W_n, V_{n-1})$の一致を検証する。同様

$$V_0 = E(A(+)A_x, S)$$
$$W_0 = E(A(+)A_x, V_0)$$
$$V_1 = E(A(+)A_x, S(+)1)$$
$$W_1 = E(A(+)A_x, V_1)$$
$$M_0 = E(W_1, V_0)$$

及び

$$V_{n'-1} = E(A(+)A_x, S(+)(n'-1))$$
$$V_{n'} = E(A(+)A_x, S(+)n')$$
$$V_{n'+1} = E(A(+)A_x, S(+)(n'+1))$$
$$W_{n'+1} = E(A(+)A_x, V_{n'+1})$$
$$M_{n'} = E(W_{n'+1}, V_{n'})$$

のように$A(+)A_x$を使い、中継サーバによる認証ステップＳ１６において$W_{n'-1}=E(A(+)A_x, V_{n'-1})$の一致と$M_{n'-1}=E(W_{n'}, V_{n'-1})$の一致を検証する。この方法によれば、ユーザは安全性を損なわずに同じパスワードＳと識別子Ａを、メールサーバとの認証処理及び中継サーバとの認証処理のどちらにも使用できるので都合がよい。

【００７２】この様に、図９の実施例では、ユーザがステップＳ６でメールサーバ１３に対しメール要求を送ってから、中継サーバ１８との接続を切断し、他のタスクに切り替えることができる。要求したメールは中継サーバとの接続切断後、数分経過してからであればいつでも中継サーバに取りにいくことができる。従って、ステップＳ６のメール要求からメールサーバで認証（ステップＳ８）後、メールが中継サーバに転送されてくるまで通信を接続したままで待機する必要はない。

【００７３】図９の実施例では、第１及び第２実施例の

28

ステップＳ１８：中継サーバは登録されているデータ$W_{n'-1}$, $W_{n'}$, $M_{n'-1}$ を$W_{n'}$, $W_{n'+1}$, $M_{n'}$ に書き換え、ｎ'をインクリメントする。

【００７１】この例では、簡単のため、ステップＳ１４における認証用データの計算に使用する識別子ＡとパスワードＳはメールサーバとの間の認証処理で使用するものと同じものを使用する場合を示しているが、パスワードは異なるパスワードＳ'を使ってもよい。その場合、中継サーバに予め登録するデータW_0, W_1, M_0も、Ｓ'を使って求めたものである。或いは、ユーザは中継サーバとの認証処理に、メールサーバとの認証処理と同じパスワードＳと識別子Ａを使用し、以下のような処理を行ってもよい。予めメールサーバ及び中継サーバの公開された識別子をそれぞれA_u及びA_xとすると、ユーザとメールサーバ間の認証処理においては、前述の初期登録のための式(1a)～(1e)及び検証のための式(2a)～(2e)において、次式

(1a')
(1b')
(1c')
(1d')
(1e')

(2a')
(2b')
(2c')
(2d')
(2e')

に、ユーザと中継サーバ間の認証処理においては、前述の初期登録のための式(1a)～(1e)及び認証のための式(2a)～(2e)における各識別子Ａの代わりに、次式

(1a")
(1b")
(1c")
(1d")
(1e")

(2a")
(2b")
(2c")
(2d")
(2e")

29

場合と同様に、ユーザとメールサーバ１３間の認証回数ｎはメールサーバ１３から与えられる場合を示した。しかしながら、図９において中継サーバが識別子Ａに対応して認証回数ｎとｎ'の両方を持っていれば、ステップＳ２，Ｓ３を省略することができる。その場合の、ｎ回目の認証処理を図１０に示す。

【００７４】図１０の例では、メールサーバは初期登録されたデータのうち、認証回数初期値n=1 を予め中継サーバに送付しておく。中継サーバには、図９の場合と同様に識別子Ａと対応させてn', W_{n-1}, W_n, M_{n-1} が登録されており、更に、ユーザとメールサーバ間の認証回数ｎも中継サーバには識別子Ａと対応させて登録されている。

【００７５】ステップＳ１でユーザから識別子Ａとメール要求を受けると、中継サーバはメールサーバにそのメール要求と識別子Ａを転送せず、ステップＳ２で直ちに識別子Ａと対応する認証回数ｎをユーザに返送する。従って、ユーザは、ｎを使ってステップＳ３で認証用データV_{n-1}, W_{n-1}, M_nを計算し、ステップＳ４でこれら認証用データを識別子Ａ及びメール要求と共に中継サーバを介してメールサーバに送り、その後、中継サーバとの接続を切断して、端末を他のタスクに切り替えることができる。ステップＳ４～Ｓ１５は、図９におけるステップＳ６～Ｓ１７と全く同様である。中継サーバはステップＳ１６で認証用データW_{n-1}, W_n, M_{n-1} をW_n, W_{n-1}, M_n に書き換え、中継サーバの認証回数ｎ'及びメールサーバの認証回数ｎをそれぞれインクリメントする。なお、認証回数ｎのインクリメントは、ステップＳ７でメールサーバから認証されたことを表す情報を受けた後であればいつ行ってもよい。

【００７６】図１０の実施例においても、図９で説明したと同様に、ユーザとメールサーバ間の認証処理には、識別子Ａの代わりに$A(+)A_n$を使い、ユーザと中継サーバ間の認証には、Ａの代わりに$A(+)A_n$を使うのが好ましい。この様に、図９及び１０の実施例では、ユーザは中継サーバ１８を用いてサービス要求とユーザ識別子Ａを中継サーバ１８に送信することにより認証手順を起動した後に、一旦中継サーバとの接続を切断する。中継サーバ１８は、ユーザから送られてきた認証用データを用いて認証者装置であるメールサーバに送り、認証処理を行い、ＯＫであれば電子メールの転送を受ける。ユーザは、しばらくして再度中継サーバと認証処理を行い、必要な情報の転送を得ることができる。

【００７７】この様な構成をとることによって、ユーザと中継サーバ間では、中継サーバが公開されているために、HTTPなどの高速転送プロトコルを用いることができる。また、中継サーバとイントラネット内部にあるメールサーバ間の通信も、ファイアウォールを回避するために電子メールプロトコルを用いるとはいえ、経由するホスト数が少ないため、転送速度を高めることができる。

30

【００７８】また、更に高速処理を実現するために、認証に用いている認証回数ｎを、メールサーバと中継サーバで共有するようにし、認証の度毎に同期をとって更新するようにすれば、認証手順を１往復削減できる。

実施例４

次に、この発明の認証方法を、インタネット上でのサービスに対する課金システムに適用した実施例を、図１１、１２を参照して説明する。近年、インタネット上でのショッピングが実現化されていくことが予想されている。これまでのインタネットショッピングでは、ユーザはインタネット上のサービスプロバイダのホームページにアクセスし、所望の商品やサービスに対し、クレジットカードでの支払いを行うのが一般である。しかしながら、クレジットカードでの支払いは１回で使用可能な最低限の金額が比較的に大きく、日常的に利用するのには不便である。しかも、利用者はクレジットカードの番号をプロバイダに送信する必要があるので、安全上問題がある。

【００７９】不特定多数のユーザは、それぞれが決めた金額＄Ｘをインタネット上に設けられた課金管理センタ２１に対し、例えば、電話などを用いて、まとめてクレジットカードで支払う。或いは、ダイアルＱ２（料金代行徴収サービス）により支払うなどの方法により、それぞれ異なるパスワードＳとアカウントＡの組が例えば郵送、或いは直接電話からメッセージで与えられる。　ステップＳ０：課金管理センタは、各アカウントＡに対して支払われた金額Ｘと、この発明による認証手順に使われる初期登録データn=1, W_0, W_1, M_0をメモリ（図示せず）に保持しておく。

【００８０】ステップＳ１：ユーザは、インタネット上のサービスプロバイダ２２のホームページなどからサービスカタログを得て、所望のサービスを指定するサービス要求信号とアカウントＡをサービスプロバイダに送信する。

ステップＳ２：サービスプロバイダはユーザのアカウントＡを課金管理センタに送り、対応する認証回数ｎを要求する。

【００８１】ステップＳ３：センタはアカウントＡに対応する認証回数ｎをメモリから読み出し、サービスプロバイダに送る。

ステップＳ４：プロバイダはJava Applet で記述されたユーザ側認証手順のプログラムと共に、認証回数ｎをユーザに送る。

ステップＳ５：ユーザはパスワードＳ、アカウントＡ、認証回数ｎを使って認証手順に従って式(2a)～(2e)を計算し、認証用データV_{n-1}, W_{n-1}, M_nを求め、ステップＳ６でサービスプロバイダに送る。

【００８２】ステップＳ７：プロバイダはユーザが指定したサービスの金額ｘと、プロバイダのアカウントA_rと共に、認証用データV_{n-1}, W_{n-1}, M_n及びユーザアカウン

31

トＡを課金管理センタに転送する。

ステップＳ８：センタは支払金額ｘがユーザアカウントＡに対応する残額Ｘ以下であるかを判定し、以下であれば図３のステップＳ５と同様に、受信したデータV_{n-1}の正当性及び登録されているデータW_nの正当性を検証し、これらが正しければ、ステップＳ９で確認信号OKをプロバイダに送信する。

【００８３】ステップＳ１０：センタは更に、登録データをW_0, W_{n-1}, M_nに更新し、認証回数ｎをインクリメントし、ユーザの残額ＸをX-x に更新する。又、プロバイダのアカウントA_iの残額X_iをX_i+xに更新する。

ステップＳ１１：サービスプロバイダは、センタからの確認信号OKを受信すると、ユーザに指定されたサービスを提供する。

【００８４】この様に、この発明の認証手順をインタネットショッピングにおける認証に適用することにより、少額な支払いも可能となり、しかも安全に決済を行うことができる。

【００８５】

【発明の効果】以上説明したように、この発明の情報送受信制御方法は、その認証手順において、被認証側にＩＣカード等の記憶媒体の読み書きを行う機構や乱数発生機構を必要とせず、小さいプログラムサイズでの処理を可能にしているため、インタネット家電のような処理能力の限られた端末に対しても、安全な情報蓄積検索サービスを提供することが可能になる。

32

【図面の簡単な説明】

【図１】従来のＣＩＮＯＮの認証手順を示す図。

【図２】この発明の第１の実施例である公衆電子メール転送サービスのシステムの概要を示す図。

【図３】第１の実施例である公衆電子メール転送プロトコルの詳細を示す図。

【図４】第１実施例におけるユーザ端末の機能ブロック図。

【図５】第１実施例におけるメールサーバの機能ブロック図。

【図６】サーバからJavaのAppletを使って提供される認証手順を使って認証手順を実行する場合にこの発明を適用した場合の初期登録手順を示すフロー図。

【図７】第２実施例におけるｎ回目の認証手順を示すフロー図。

【図８】インタネット上の中継サーバを介してメールサーバにアクセスする場合にこの発明を適用した第３実施例のシステム図。

【図９】図８のシステムにおいて、第３実施例による認証手順を示すフロー図。

【図１０】第３実施例の変形実施例を示すフロー図。

【図１１】この発明による認証方法をインタネットショッピングに適用した場合のシステムズ。

【図１２】この発明の認証方法が適用されたインタネットショッピングの手順を示す流れ図。

【図１】

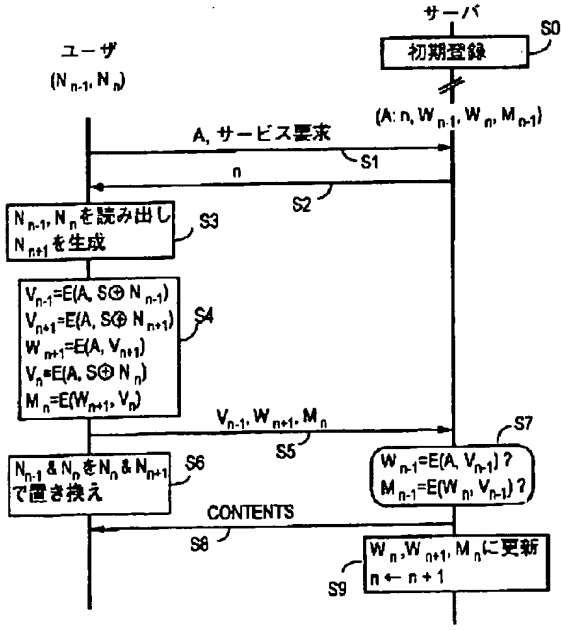


図1

【図３】

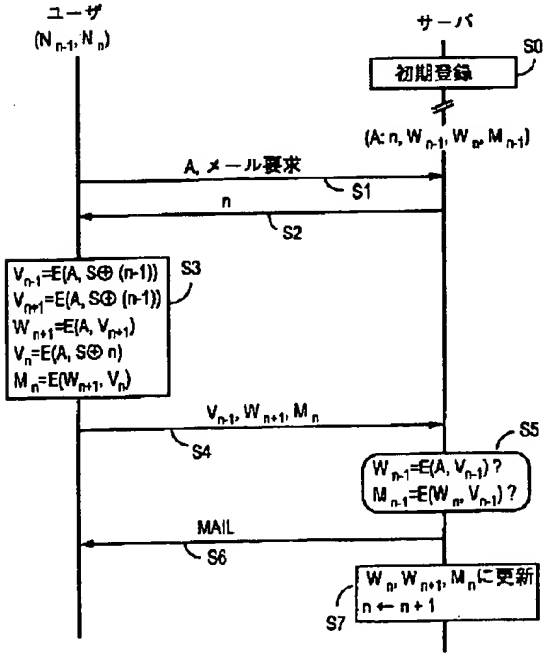


図3

【図２】

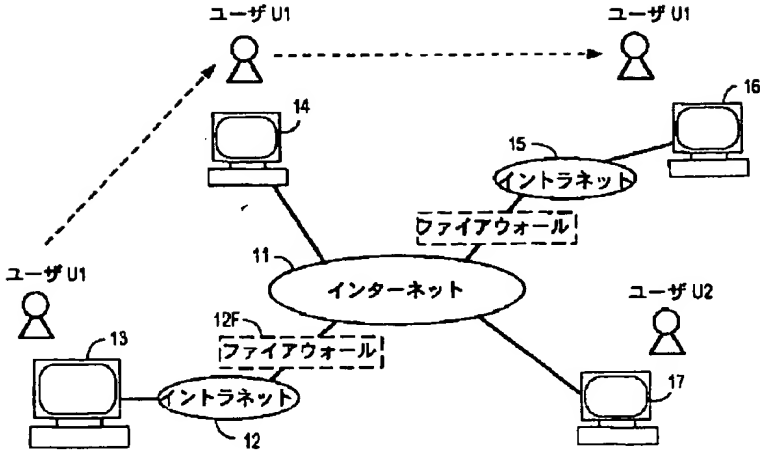


図２

【図４】

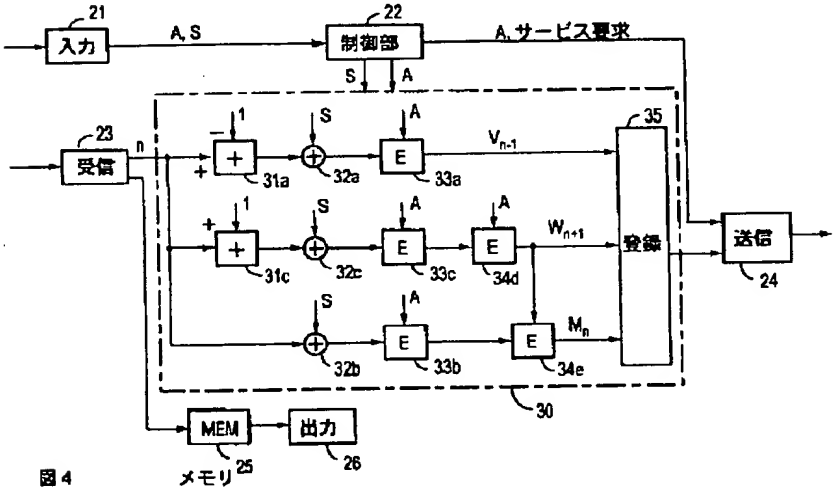


図４

【図８】

【図１１】

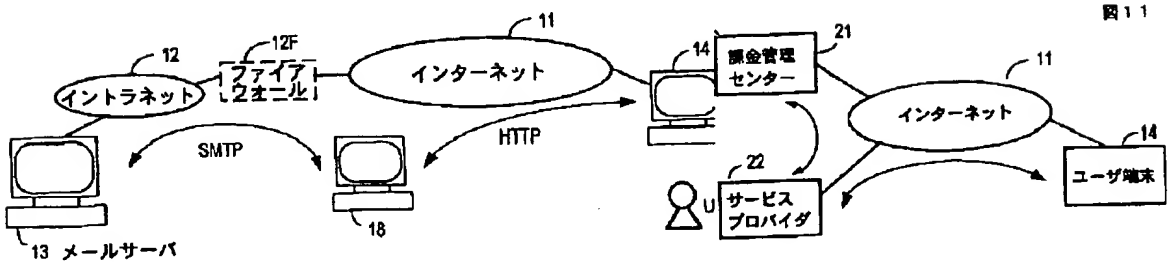


図１１

図８

【図５】

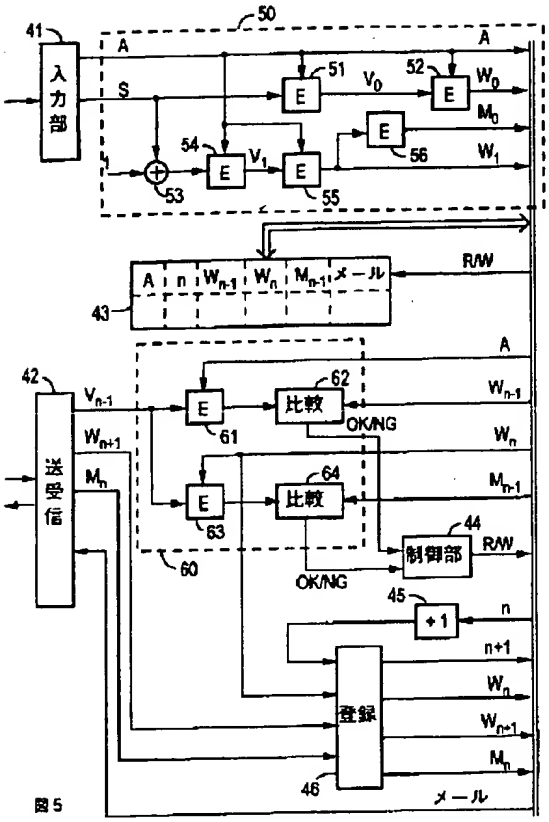


図５

【図６】

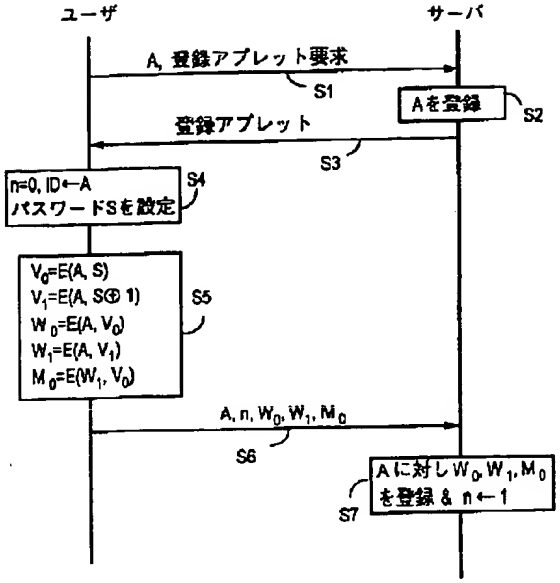


図６

【図７】

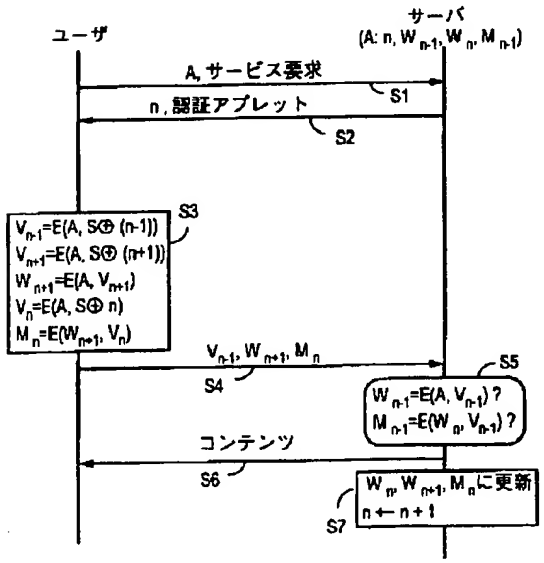


図７

【図９】

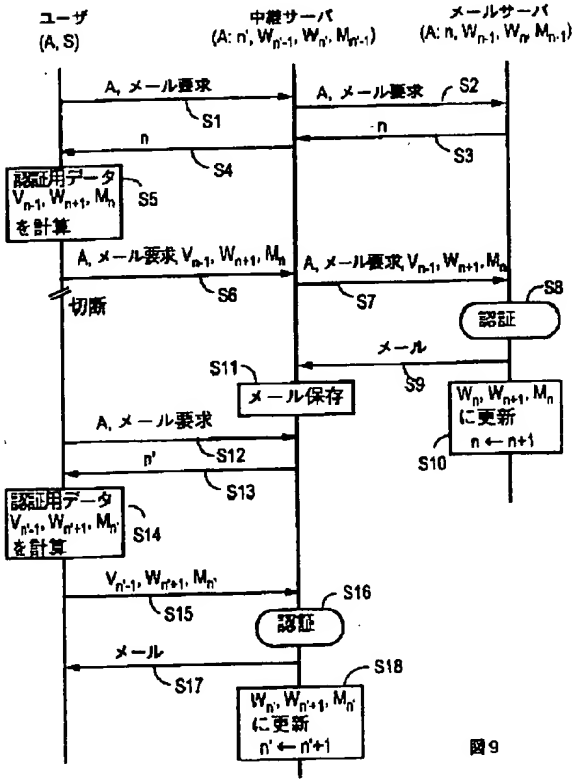


図９

【図１０】

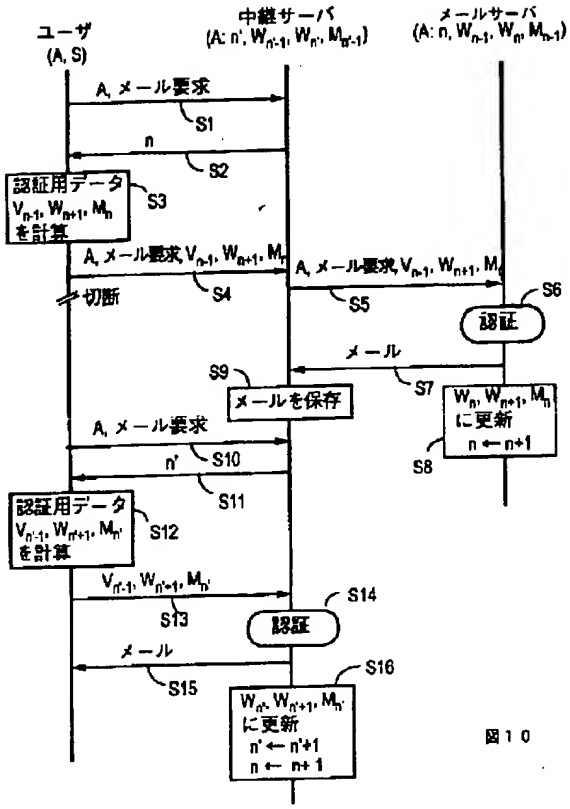


図１０

【図１２】

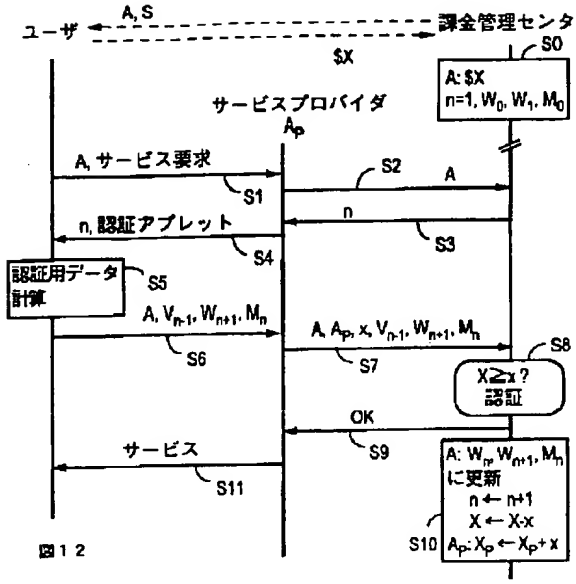


図１２